THE TRUE IDENTITY OF AUSTRALIAN IDENTITY THEFT OFFENCES:A MEASURED RESPONSE OR AN UNJUSTIFIED STATUS OFFENCE?

ALEX STEEL*

I INTRODUCTION

Much has been written about identity theft, with many making hyperbolic claims that it is the 'fastest growing crime in the world' or the 'crime of the millennium'.[1] In the last few years, Australian jurisdictions have felt the need to enact offences that are described as identity theft or identity crime offences, and are specifically targeted to deal with this phenomenon by prohibiting the possession of personal information with intent to commit further crimes. This poses the question whether such laws are properly framed and amount to a measured response to a new criminal phenomenon, or whether they are instead overly broad and in violation of fundamental legal principles.

This article provides an analysis of those new laws.[2] After defining what is meant by identity theft and identity crime it provides an overview of some of the differences in the nature of digital crime that have led to calls for specific legislation, and some of the problems that face traditional approaches to investigating and preventing fraud. It goes on to examine the specific approaches taken in Australian identity theft law, considering whether the prohibited subject of the offences – identification information – is defined too widely. The core behaviour prohibited – possession – is then examined in detail. The article argues that possession is an inappropriate basis for criminalisation on both theoretical and practical grounds, and illustrates this by a comparison with the concept's use in insider trading and child pornography offences. Similar issues are raised with the 'dealing in information' offence.

---

* Associate Professor, Faculty of Law, University of New South Wales. Many thanks to Alana Maurushat for comments on an early draft, the anonymous referees, and James Dorney for research assistance.

1 See, eg, Holly K Towle, 'Identity Theft: Myth, Methods and New Law' (2004) 30 *Rutgers Computer & Technology Law Journal* 237, 238 citing Stephen F Miller, 'Someone Out There Is Using Your Name: A Basic Primer on Federal Identity Theft Law' (2003) 50(1) *Federal Lawyer* 11; Sean B Hoar, 'Identity Theft: The Crime of the New Millennium' (2001) 80 *Oregon Law Review* 1423.

2 Due to space considerations this article does not discuss the possession of equipment for the manufacturing of false identities offences. These offences also raise concerns about over-criminalisation.

It is argued that the inadequacies of these provisions are the outcome of an approach to law making that creates criminal liability too early in the chronology of planning and executing crime. As a result the offences fail to exhibit sufficient external elements to satisfy fundamental requirements of the rule of law, and place too much unfettered discretion in the hands of law enforcement.

II CRIME IN HYPERSPACE

A Defining Identity Crime

Disagreement still exists over what identity theft actually is and its relationship to identity crime in general. Broadly, identity crimes can be described as crimes that are in some way enabled by the use of an identity that is not the identity of the perpetrator. The most commonly understood form of identity crime is that of identity fraud, where the perpetrator uses an alternative identity[3] to obtain benefits, and where the victim is induced to accept that this alternative identity is in fact the perpetrator's true identity. Within these broader concepts, identity theft is often used to describe the preparatory act of acquiring the personal identification information or accreditation of a third party victim, in order to allow this to be used as an alternative identity in a crime. Looser use of the term extends to any crime committed with the alternative identity. This broader use aims to describe the sense of violation the third party victim feels, and the financial liability or other consequences that are attributed to them as a result of the fraudulent use of their identification information.[4] In this article the term will be used to describe the acquisition and retention of identification information, rather than any further use to which that information is put.

B The Phenomenon of Hyperspace

Identity based crimes are nothing new. Most fraud involves some form of manipulation of identity. This manipulation can occur through words or conduct, and often via misleading written statements and images.[5] However, it is generally accepted that the pervasiveness of email and the internet in the last decade has made possible the commission of identity based crimes on a scale until now unimaginable.[6] There are a number of reasons for this. The global reach and extraordinary speed of digital networks and electronic commerce mean we now

3 I use this term to describe both situations where the identity is appropriated from another person, as well as where it is entirely or partially fictitious.

4 For discussion of these terms see, eg, Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step towards Consistency* (2006).

5 See, eg, the definition of deception in the *Crimes Act 1900* (NSW) s 192B.

6 For a comprehensive analysis of this phenomenon, see David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge University Press, 2007).

inhabit a world that McGuire terms 'hyperspace'.[7] Details can be transmitted and transactions can occur instantaneously, and we no longer have a sense of physical distance about such communication and interaction. An electronic transaction between Sydney and Eastern Europe takes as long as one between persons in Sydney, and both are significantly faster than transacting in person at the local post office. Today, the post office is in a real sense much further away (in travel time and effort) than the 'shopping cart' on our computer browser. Not only does this put us in touch with the world, but the world is also in touch with us.

As well, the internet is a means by which we can represent ourselves to any place or places in the world – and can do so from any other place. At almost no cost we can appear in the email inboxes or internet browsers of hundreds or even millions of people internationally and instantaneously. In this sense the internet is a force multiplier. One act can create multiple communications for minimal cost. Whereas a mail based fraud involves the cost of stationery and stamps with each letter sent – and the volume of letters sent could be easily detected – spam emails only require a mailing list.

With this virtually no-cost distribution of fraudulent misrepresentations come two further factors. First, the aggregation of information on the internet, both in databases and as a result of internet searches, has meant the creation of many data rich sites that can provide highly efficient places from which to gather data that assists the perpetration of fraud. This data can also be accessed remotely and anonymously (sometimes even legitimately). Examples are the databases of international credit card organisations and social networking sites.

Secondly, that the internet makes feasible what David Wall terms 'micro-crimes'. These are crimes that are only made economically feasible due to the force multiplier effect. An elaborate scam that nets a result of only a few cents becomes viable if it can be repeated thousands of times; a scam that only cons one in a thousand people becomes highly successful if hundreds of thousands are emailed worldwide.[8]

Finally, the ability to access much of this data and to perpetrate the frauds remotely renders these crimes attractive to those who might be deterred by the physical risks of face to face crime. There is arguably less perceived risk of personal injury in an online fraud compared to, say, a bank robbery. This suggests that there is consequently a greater range of people who might be attracted to internet based crimes and that such crimes can be an attractive exploit for young people.[9]

---

7 Michael McGuire, *Hypercrime: The New Geometry of Harm* (Routledge-Cavendish, 2007) 6. McGuire uses this term in contrast to 'cyberspace' to emphasise that the social construct of modern life involves both online and real world elements.

8 See David S Wall, 'Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age' in Thomas J Holt and Bernadette H Schell (eds), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Information Science Publishing, 2010).

9 Cf Majid Yar, 'Computer Hacking: Just Another Case of Juvenile Delinquency?' (2005) 44 *The Howard Journal of Criminal Justice* 387.

Internet technologies allow us to create highly extenuated forms of identity. The severe disjunct between our physical presence and our represented presence, or 'telepresence',[10] allows us a high degree of control over how we represent ourselves. None of our actual physical characteristics or circumstances need be transmitted, and alternatives can be readily substituted.[11] Previous constraints on the believability of impersonators, which required innate abilities or the learning of a craft, no longer apply. Physical cues, such as nervousness, ability to speak the language, as well as age and gender can all be more easily disguised in a largely text based form of identity.

The speed at which information is processed online also makes us impatient with delay, and we expect transactions – anywhere in the world – to be completed almost instantaneously. This impacts on the ability of transactors and intermediaries to properly verify identities in acceptable timeframes. Additionally, the novelty of online communication and transaction has resulted in a significant gap in consumer education, allowing for a high degree of gullibility in accepting that internet representations are indeed as they appear.[12]

All of these technologically based developments in personal identity and representation can be misused and used to perpetrate identity based crime. The malleability of online identity, and the speed at which it can be transmitted, in multiple forms and on an international scale, causes great fear to many. Such fears often involve the spectre of a person impersonating one's identity, draining one's bank accounts, racking up credit card debts, and even committing crimes in one's name. Marron summarises the result:

> The contemporary conception of identity theft, then, is that of a technological rollercoaster of hyper-fast markets and light-speed information assembly – a 'disorganized capitalism' which helps to fulfil consumerist dreams and ambitions and yet, at the same time, opens the possibility of exactly their opposite: denial, inhibition and a state of unfreedom seemingly unlimited in time and space. It is this 'worst case scenario' that becomes the baseline by which identity theft is conceptualized and acted upon.[13]

It is however important to recognise that the vast majority of online interactions are not fraudulent. A great deal of technological innovation goes towards ensuring the security of online transactions and while the risk of online fraud is real, overwhelmingly the world has embraced e-commerce as efficient and reliable. There continue to be problems in properly assessing the extent of internet based crime, with ongoing issues of data verification.[14] However, this 'worst case scenario', as outlined by Marron, leads to pessimistic interpretations of the situation, and a sense of online fraud reaching epidemic proportions.

---

10 McGuire, above n 7, 28 citing Marvin Minsky,'Telepresence' (1980) 2(9) *Omni* 45.

11 See, eg, Peter Steiner, 'On the Internet, Nobody Knows You're a Dog' 69(20) *The New Yorker* 61.

12 See generally House of Representatives Standing Committee on Communications, Parliament of Australia, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime* (2010) 55–6.

13 Donncha Marron, 'Alter Reality: Governing the Risk of Identity Theft' (2008) 48 *British Journal of Criminology* 20, 25.

14 See Wall, above n 6, 13–29. Recent international and Australian data sources are set out in Hackers, Fraudster and Botnets, above n 12, 31–4.

C The Impact on Law Enforcement

The hyperspatial nature of identity appropriation also causes problems for law enforcement. Traditional methods of dealing with craft based fraud involve police exploiting the long period of time taken in planning such frauds. This can allow police to engage in surveillance and infiltration of known fraudsters, or to follow forensic clues left by the perpetrators.[15] Such techniques are much more difficult to apply to online fraud detection. Automated crime involving international transactions essentially requires automated detection and international agencies. The costs of developing and training officers to use computerised investigation technologies is considerable, and blanket surveillance techniques raise concerns regarding civil liberties and freedom of speech.[16] The international aspect of these crimes also raises difficulties in arranging international law enforcement cooperation – not the least of which is differing national legal regimes.[17]

Despite the creation of specialist agencies,[18] and attempts to reconceptualise the notion of policing, police forces remain strongly terrestrial and organised around the physical control of individuals.[19] This means that whereas internet based crimes might be seen to be widespread, the numbers of officers who are expert in their investigation are small. These difficulties have led to the enactment of a range of laws internationally that seek to make it easier for law enforcement bodies to prosecute those involved in identity theft.

Where offences are seen to be commonplace or difficult to investigate in detail, police forces have historically relied on 'sweep' offences – offences that give broad discretion to police to arrest people they suspect are engaged in criminal activity on the basis that they fall within a particular status of undesirable characters. Historically, such offences developed out of customary or common law powers of police or magistrates and were restated as offences when codified.[20] Such sweep offences are largely discredited in modern legal

15 A well known example of these classic techniques is the way in which Frank Abagnale was apprehended: Frank W Abagnale, *Catch Me if You Can* (Broadway, 2000).

16 See, eg, Daniel Solove, 'Reconstructing Internet Surveillance Law' (2004) 72 *George Washington Law Review* 1264; David Lyons (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing, 2006).

17 See Susan W Brenner and Joseph J Schwerha IV, 'Cybercrime Havens: Challenges and Solutions' (2007) 17 *Business Law Today* 49; Roderick Broadhurst, 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29 *Policing: An International Journal of Police Strategies & Management* 408. The Australian perspective is outlined in Standing Committee, above n 12, 68–71, 114–22.

18 Cf McGuire, above n 7, 265–71.

19 Cf Laura J Huey, 'Policing the Abstract: Some Observations on Policing Cyberspace' (2002) *Canadian Journal of Criminology and Criminal Justice* 243. Current Australian policing issues are outlined in Hackers, Fraudster and Botnets, above n 12, 72–93.

20 David Dixon, *Law in Policing: Legal Regulation and Police Practices* (Clarendon Press, 1997) 68 ff.

commentary[21] and there have been recommendations by Law Reform bodies for their repeal,[22] though there has been something of a renaissance in their use within terrorism offences.[23] Offences such as vagrancy, loitering and consorting are the more obvious of the sweep offences,[24] but it has been argued that possession offences are the modern equivalent.[25] As we will see, the approach to policing of identity theft falls back onto these general possession offences as the main method of law enforcement. Whether this is a realistic acknowledgment of the inability of law enforcement to police the internet or an attempt to create short cuts in criminalisation is ultimately a moot point.

III AUSTRALIA'S NEW 'IDENTITY THEFT' OFFENCES

Australia now has specific identity offences in the five largest State jurisdictions and a Bill on the issue currently before the Commonwealth Parliament.[26] South Australia's offences were enacted first, in 2003.[27] Queensland followed in 2007.[28] Both approaches were considered in a 2008 report of the Model Criminal Law Officers Committee ('MCLOC', formally known as 'MCCOC'),[29] which proposed a set of offences similar to those enacted in Queensland. A modified form of these recommendations was introduced into the Commonwealth Parliament in 2008[30] and passed by the House of Representatives without amendment or the need for a division.[31] It was still awaiting debate in the Senate when Parliament was prorogued for the 2010

21 See, eg, Markus Dirk Dubber, 'The Possession Paradigm: The Special Part of the Police Power Model of the Criminal Process' in Antony Duff and Stuart P Green (eds), *Defining Crimes: Essays on the Special Part of the Criminal Law* (Oxford University Press, 2005); Tim Newburn and Robert Reiner, 'Policing and the Police' in Mike Maguire, Rod Morgan and Robert Reiner (eds), *The Oxford Handbook of Criminology* (Clarendon Press, 1994); Alex Steel, 'Consorting in New South Wales: Substantive Offence or Police Power?' (2003) 26 *University of New South Wales Law Journal* 567.

22 See, eg, Law Reform Commission of Western Australia, *Police Act Offences*, Project No 85 (1992); Scrutiny of Acts and Regulations Committee, Parliament of Victoria, *Review of the Vagrancy Act 1966: Final Report* (2002).

23 See, eg, Bernadette McSherry, 'Terrorism Offences in the Criminal Code: Broadening the Boundaries of Australian Criminal Laws' (2004) 27 *University of New South Wales Law Journal* 354.

24 See David Brown et al, *Criminal Laws: Materials and Commentary on Criminal Law and Process in New South Wales* (Federation Press, 4th ed, 2006) 834–50.

25 Dubber, above n 21, 96.

26 The proroguing of Parliament in July 2010 led to the Bill lapsing; at the time of publication it has not been re-introduced.

27 *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA).

28 *Criminal Code and Civil Liability Amendment Act 2007* (Qld).

29 Model Criminal Law Officers Committee of the Standing Committee of Attorneys-General, *Final Report: Identity Crime* (2008). This followed on from an earlier reports into credit card skimming offences: Model Criminal Code Chapter 3 Discussion Paper: Credit Card Skimming Offences; Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Final Report: Model Criminal Code: Chapter 3 Credit Card Skimming Offences* (2008).

30 Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 (Cth).

31 Commonwealth, *Parliamentary Debates*, House of Representatives, 23 February 2009, 1458.

election. NSW introduced its own laws in 2009,[32] which are largely similar to the Model Criminal Code proposals.[33] Victoria's 2009[34] and Western Australia's 2010[35] legislation are further variations of the Model Criminal Code version.

While there are important differences between the wording of the offences, discussed below, there is a fundamental agreement about the underlying definitions and type of behaviour prohibited. The form the legislation takes appears to be a response to two key difficulties that law enforcement has faced in prosecutions in this area. The first is in describing the nature of information or material that can be used to validate identity. The second is the impact digital networks have had on the speed with which such offences can be committed and the concomitant ability to perpetrate such offences remotely and on multiple targets simultaneously.

The legislation deals with these issues in two ways. First, the offences enact a very broad scope of proscribed behaviour. Secondly, they move the time at which behaviours crystallise into an offence to a point significantly earlier than is the case for traditional offences. The effect of both characteristics is to place a heavy emphasis on the mental elements of the offence as the differentiator between lawful and criminal behaviour.

A Identification Information

All of the legislative schemes prohibit unlawful behaviour in relation to 'identification information'.[36] This is described broadly in all schemes as 'information relating to a person … that is capable of being used … to identify or purportedly identify the person'.[37] This is followed by a long indicative list of possible forms of identification information. There are some minor differences between jurisdictions in the contents of these lists, but as they are inclusive the differences are not significant. A representative set is contained in the NSW scheme: [38]

> ***identification information*** means information relating to a person (whether living or dead, real or fictitious, or an individual or body corporate) that is capable of being used (whether alone or in conjunction with other information) to identify or purportedly identify the person, and includes the following:
>
> (a) a name or address,
>
> (b) a date or place of birth, marital status, relative's identity or similar information,
>
> (c) a driver licence or driver licence number,
>
> (d) a passport or passport number,

32 *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009* (NSW).

33 The significant difference relates to the scope of the possession of equipment offences. These are not discussed in this article, but are themselves of concern.

34 *Crimes Amendment (Identity Crime) Act 2009* (Vic).

35 *Criminal Code Amendment (Identity Crime) Act 2010* (WA).

36 South Australia terms it 'personal identification information'.

37 Queensland uses 'entity' instead of person.

38 *Crimes Act 1900* (NSW) s 192I.

(e) biometric data,
(f) a voice print,
(g) a credit or debit card, its number or data stored or encrypted on it,
(h) a financial account number, user name or password,
(i) a digital signature,
(j) a series of numbers or letters (or both) intended for use as a means of personal identification,
(k) an ABN.

What is striking is that the lists are not limited to private information or secret passwords. Instead, the lists include types of data that are publicly available and often well known, like a person's name and address, date and place of birth, and marital status. For most celebrities and many people with social networking websites, all of this information is readily accessible on the internet. Similarly, the signatures of many can easily be found on the internet as parts of letters, submissions, personalised websites, and so on.[39]

The result is that identification information is neither necessarily restricted nor private information. Indeed there is nothing unlawful in being aware of such information, nor need there be any consent granted for its wide public distribution.[40] The situation is even more extreme for corporations. As legal entities, corporations fall within the scope of 'persons' covered by this legislation.[41] Thus ABNs, corporate addresses and phone numbers would all fall within the scope of 'identification information'. There are in fact legal requirements that much of this information be publicly available.[42]

B The Intent with Which Identification Information Is Possessed

Conspicuously, the offences do not attempt to describe or prohibit the act of 'identity theft'. Instead they concentrate on a concept of possession of information and further general criminal intention in relation to that information. Thus, all the legislative schemes make it an offence to be in possession of 'identification information'[43] with

- an intention of committing, or facilitating the commission[,] of an indictable offence (NSW);[44]

39 It is worth noting that the term 'digital signature' is not defined in all jurisdictions. In those where it is, such as Western Australia, it is limited to encrypted combinations of numbers and letters: see, eg, Sharon Christensen et al, 'The Statute of Frauds in the Digital Age – Maintaining the Integrity of Signatures' (2003) 10(4) *Murdoch University Electronic Journal of Law* 44 <http://www/murdoch.edu.au/elaw/issues/v104/christensen104.html>.

40 The legislation in some jurisdictions makes clear that consent is irrelevant: see, eg, *Crimes Act 1958* (Vic) ss 192B, 192C(3).

41 *Acts Interpretation Act 1987* (Cth) s 21.

42 See *Corporations Act 2001* (Cth) ch 2C: public registry requirements.

43 In South Australia it is 'prohibited material' under s 144A of the *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA). This is a functional definition that includes 'personal information'.

44 *Crimes Act 1900* (NSW) s 192K.

- [an intention that] any person … will use the identification information to pretend to be, or to pass the user off as, another person … for the purpose of … committing [or facilitating] an [indictable] offence (Cth);[45]
- the purpose of committing, or facilitating the commission of, an indictable offence … (Qld);[46]
- inten[t] to use the material … in [committing, or facilitating the commission of, an offence] (SA);[47]
- intention that the material will be used … to commit [or facilitate] an indictable offence … (WA);[48]
- inten[t] to use … the information to commit an indictable offence, or to facilitate the commission of an indictable offence (Vic).[49]

When listed, it becomes clear that the proposed Commonwealth offence is more tightly expressed than the offences in other jurisdictions. The Commonwealth offence will require the prosecution to establish that the 'identification information' is intended to be used to impersonate or create a false identity in order to facilitate a crime – ensuring a fraud basis to the offence. The offences in the other jurisdictions do not. This means that in NSW, Queensland, South Australia, Victoria and Western Australia it is a crime to possess the address details of a bank that one intends to rob. One consequence of the lack of restriction in these states is that there is now, at least in theory, an additional offence committed in all planned crimes as a result of recording or being aware of the details of the target – individual or corporation.

Previously, liability would arise in the case of conspiracy to rob, an attempted robbery, or a completed robbery. In five Australian jurisdictions there is now an additional 'back-up' charge of possessing the address of the target bank.

The South Australian offence is the broadest of all. That scheme employs the term 'prohibited material', which includes personal information, but also extends to 'anything that enables a person … to exercise a right of ownership that belongs to someone else to funds, credit, information or any other financial or non-financial benefit'.[50] This definition is astoundingly wide. It goes beyond information to include tangible property. There are a range of rights of ownership, which can be as minor as access or use rights. Non-financial benefits could include a sense of well being. When the elements are combined, the possession offence is broad enough to criminalise the possession of keys to buildings or vehicles that a person intends to unlawfully enter or use for almost any benefit. This is not to suggest that possession of things such as housebreaking implements should not be criminalised,[51] but that it is

45 Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 sch 1 pt 1 cl 372.2.

46 *Criminal Code Act 1898* (Qld) s 408D(1); 'obtaining' includes possessing: at s 408D(7).

47 *Criminal Law Consolidation Act 1935* (SA) s 144D(1)(b).

48 *Criminal Code Amendment (Identity Crime) Act 2010* (WA) will insert a new section 490 into *Criminal Code Act Compilation Act 1913* (WA); 'material' is defined in section 489 as information or a record containing that information.

49 *Crimes Act 1958* (Vic) s 192B(1)(b).

50 *Criminal Law Consolidation Act 1935* (SA) s 144A.

51 They have long been the subject of criminal offences: see, eg, *Crimes Act 1900* (NSW) s 114.

inappropriate to extend an offence in a part entitled 'Identity Theft'[52] to cover such activities.

Most of these difficulties arise because of the protean nature of the prohibited activity. The key to individual identification is to describe that individual in a way that is unique to them. The most basic method is the attempt to give each person a unique name. This quest for uniqueness inevitably leads to constant innovation and invention in methods of description – biographical data, passwords, biometric data, identification numbers or combinations of these. This evolving and fluid combination of identifiers presents an impossible task of definition for the criminal law and so the legislative response has instead been to allow almost anything to comprise identification information. This creates an over inclusive definition that catches forms of identification that are nowhere else restricted or seen to be private or sensitive.

IV THE INAPTNESS OF THEFT AND POSSESSION AS CONCEPTUAL BASES FOR IDENTITY CRIME

A Theft: A Crime with Its Basis in Possession

What is really at stake here is the failure of legislatures and law enforcement to properly describe the behaviour that they seek to criminalise. The offences are often described as theft[53] and, while no elements of theft are in fact prohibited, the notion of stealing identity seems to underpin much discussion of the offences. However the analogy is inappropriate.

Theft (or larceny)[54] at common law was restricted to tangible property. The elements of the crime included: that the property was physically removed from the victim's possession; that this occurred without the victim's consent; and that the perpetrator did this with the intention of permanently depriving the victim of the property.[55] Thus the offence assumed that the property in question could only be possessed by one person at a time and any use of it was exclusively controlled by the victim.[56] This highlights the artificiality of naming criminal misappropriation identity 'theft', in that the misuse of another's identity need not involve property, or material exclusively controlled by the victim. Further, in most cases there is neither removal nor deprivation relating to that material. Usually, there is instead a copying of the material. A victim of identity theft loses

52 *Criminal Law Consolidation Act 1935* (SA) pt 5A.

53 The US legislation is titled the *Identity Theft and Assumption Deterrence Act 1998*, Pub L No 105-318, §112 Stat 3007. The South Australian amending Act was entitled the *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA).

54 Larceny remains law in NSW, supplemented by legislative expansion. It has been replaced with statutory formulations in all other Australian jurisdictions.

55 *Ilich v The Queen* (1987) 162 CLR 110. Other elements, not relevant to the current discussion, are the need for a fraudulent taking without a claim of right. For more detailed discussion see Brown et al, above n 24.

56 For a detailed discussion of the elements of larceny see Brown et al, above n 24, 981–1008.

nothing when their identity is appropriated.[57] Any loss that occurs is instead associated with the illegitimate use to which their copied identity is subsequently put.

The nature of the identity descriptors acquired by the identity thief may not in fact be owned or exclusively controlled by the victim. For example, an employee's staff number identifies that person for some purposes, but is not in any sense 'owned', 'possessed' or 'controlled' by the employee. A person's residential address amounts to a description of where that person lives, but is both publicly available and not the sort of information that can be subjected to any use restrictions – such as through copyright. Doctrinally, the law has trouble proscribing or controlling information in general. Theft has always been restricted to theft of property, and information is not seen to constitute a form of property[58] other than when contained within particular forms and as defined by specific and limited legislative enactments – such as patents and copyrights.[59] There are also strong political ideologies in favour of freedom of expression that militate against blanket controls, particularly if the information is not private in nature. Thus, not only is the analogy with acquisitive crimes inapt, but serious difficulties arise over whether there is any existing legal basis for criminalising knowledge or control of information at all.

Consequently, acquisition based crimes predicated on a loss to the victim are inapt to describe acts of identity theft. This much has been acknowledged by MCLOC and the offences developed subsequent to that report are referred to as identity 'crimes' rather than identity 'theft', as is the case in South Australia.

Despite the move to cease labelling the offences as identity 'theft', the concepts underlying the identity offences remain strongly based in a sense of unlawful acquisition of personal property. This is most clearly seen in the use of the term possession and in the need felt in some jurisdictions to exclude a defence of consent to possession.[60]

B The Doctrinal Basis of Possession Offences

Not only is theft an ill suited basis for the identity crime offences, but the status that is prohibited – possession – is inappropriately derived from property law, and is both practically and theoretically suspect. An examination of the unique aspects of possession offences reveals this.

The legal meaning of possession is complex, largely due to its long use in the common law and its wide adoption in statutory offences. This means courts have

---

57 That is not to deny that a victim may suffer harm to well-being and privacy.

58 *Oxford v Moss* (1979) 68 Cr App R 183.

59 For discussion of this in a theft context see Alex Steel, 'Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property' (2008) 30 *Sydney Law Review* 575.

60 See Victorian and Western Australian offences. The exclusion of a defence of consent implies that the person consenting has the right to exclusive control over the information, and such common law rights of control would by default be proprietarily based. This can be contrasted with the limited non-proprietorial protection granted to confidential information which is removed if the information ceases to be confidential: see, eg, *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414.

felt compelled to caution that: 'the term "possession" … always giv[es] rise to trouble, and … in each case its meaning must depend on the context in which it was used'.[61]

However, there is a core meaning to possession to which all variants relate. This revolves around property and control.[62] The Canadian Supreme Court has recently held that interpreting possession in digital pornography cases must start with an understanding of possession as based around a notion of control traditionally associated with tangible objects.[63] So it is important to preface a discussion of these offences with an overview of these core notions of possession in legal discourse. Having done this, the application of possession to identification information can be considered.

At common law, possession is proved by establishing both that the person has physical control of an item and also an intention to possess that item. However, physical possession need not require continual physical capture, as in the wearing of a watch, but extends to the placing of an item in any place whence it can be retrieved. Possession continues to vest in the original owner until either another person intentionally takes over possession or the possessor clearly repudiates ongoing possession.[64] The acquisition of possession thus requires an act,[65] but the ongoing possession need not.

The physical elements of offences can be generally seen as either conduct – often in defined circumstances – or consequence offences.[66] Assault is a conduct offence in that liability lies in unlawful physical contact or the threat to make such contact. Murder is a consequence offence because the victim must die before liability arises. Possession is neither. The accused need not engage in any conduct – the actus reus element of physical control is essentially passive, and indeed can be constructive, such as when items are found in a house or a vehicle controlled by the accused. As well, there is no need to prove any consequence: possession is liability in itself. Possibly for this reason possession was never recognised as an offence by the common law.[67]

Possession is a complete offence that creates culpability prior to the point of liability of traditional inchoate offences. Attempt, for example, requires that the accused commit some act that is a substantial step towards another offence and that be unequivocally an act of perpetration of that offence.[68] By contrast, possession does not require proof of any connection with another offence. As Markus Dubber notes, possession is a conduct-less offence: it is a

---

61 *Warner v Commissioner of Police of the Metropolis* [1969] 2 AC 256, 304 (Lord Pearce) citing *Towers & Co Ltd v Gray* [1961] 2 QB 351, 361 (Lord Parker CJ).

62 One relevant example is in the *Crimes Act 1900* (NSW) s 7, which is entitled '"Possession" when criminal' and which refers exclusively to issues of custody or control of property.

63 *R v Morelli* [2010] 1 SCR 253, [18], [137]; cf *Clark v The Queen* (2008) 185 A Crim R 1, 51–4.

64 See, eg, Frederick Pollock and Robert Samuel Wright, *An Essay on Possession in the Common Law* (Clarendon, 1st ed, 1888); *Gatward v Alley* (1940) 40 SR (NSW) 174, 180 (Jordan CJ).

65 Cf *R v Michael Preston* (1851) 2 Den 35.

66 See for example the taxonomy of offences employed in *Criminal Code Act 2005* (Cth) pt 2.2.

67 See *R v Heath* (1810) Russ & Ry 184; 168 ER 750; *Dugdale v R* (1853) 1 E & B 435.

68 See, eg, *R v Mai* (1992) 26 NSWLR 371.

> ... status, or more precisely, a relationship between a person and an object. ... Rather than criminalizing future or past conduct (use or distribution and acquisition), possession punishes present status as evidence of that future or past conduct.[69]

In other words, when an offence prohibits possession of information it is really aimed at prohibiting the acquisition and/or use of information, but in doing so instead criminalises a status ancillary to either act. There is judicial authority to the same effect. In *R v Grant*, Mahon J held:

> [T]o be in possession or to have an article in possession is neither an act nor omission. It represents not an act but the passive consequences of a prior act, namely, the act of acquisition of possession[.][70]

Dubber argues that 'possession is an incapacitationist tool for the elimination of threats':[71] it is the threat that justifies the crime and thus the incapacitation. Unless the dangerousness lies in the possessor, it must lie in the object possessed. Illicit drugs, guns and child pornography are all seen to be dangerous objects. So dangerous, in fact, that their mere possession creates presumptive criminality.[72] It follows, then, that the justification of an offence of possession of information must be that the information is so inherently dangerous that society is confident that any person who has this information is likely to be involved in serious criminality.

The current blanket description of identification information fails this test of inherent dangerousness. If one considers the spectrum of sets of data that could possibly be involved in breaches of these provisions it is clear that there is not only a wide variety of the types of data that can be acquired, but also a range of possible characteristics of that data – such as particular combinations of data types or the number of distinct sets of identities involved. Dangerousness would depend on consideration of all these factors. At one end of this spectrum the obvious dangerousness of the information might be evident, but at the other end it might appear innocuous. There is thus no clear justification for the criminalisation of possession of identification information.

The reliance on this broad notion of possession as the core of the offence contrasts with the Commonwealth offences concerning personal financial information.[73] These offences primarily prohibit the dishonest acquisition or dealing in financial information.[74] Section 480.4 of the Commonwealth *Criminal Code* enacts:

---

69 Dubber, above n 21, 103.
70 (1975) 2 NZLR 165, 169.
71 Dubber, above n 21, 114.
72 See also George P Fletcher, *Rethinking Criminal Law* (Little Brown, 1978) 197–202.
73 For analysis of the offences see Brown et al, above n 24, 1040–2.
74 *Criminal Code Act 1995* (Cth) s 480.4.

480.4 Dishonestly obtaining or dealing in personal financial information

A person is guilty of an offence if the person:

(a) dishonestly obtains, or deals in, personal financial information; and

(b) obtains, or deals in, that information without the consent of the person to whom the information relates.

Penalty: Imprisonment for 5 years.

The basis of criminality in this offence is a positive act of acquisition or disposal, and that act is coupled with a requirement that the action be dishonest. 'Dishonesty' is defined in section 480.2 as being 'knowingly dishonest according to the standards of ordinary people'. In other words, acquisition or disposal of information is only criminal if the accused is aware that ordinary people would consider the actions wrong. If ordinary people do not see the behaviour as wrong, or if the accused was genuinely unaware of such a community standard, no offence is committed.

Thus, the offence first identifies two discrete acts, either of which are prohibited, and secondly requires that at the time of that act the accused is aware that such an act runs against community standards. This both ensures that there is proof of a positive and deliberate act by the accused, and also recognises that in this area there may well be a range of acceptable practices that will need to judged on a case by case basis through the application of community standards. By contrast, the identity offences fail to criminalise the very act they aim to prohibit – the acquisition of personal information – just as they fail to provide any mental element relating to any act of the accused. Instead the actus reus of the offence is the passive maintenance of a status of possession, and the mens rea is an un-acted on intention relating to future acts.[75]

C The Inappropriateness of Possession as a Conceptual Basis for Identity Crime

Possession offences are fundamentally based on tangible property. One is in possession of an object if one maintains physical control over it. Consequently, inherent in the notion of possession is the ability to lose possession as a result of any other person taking exclusive control of the item at any time.[76] The tort of conversion and the crime of larceny centre on this idea, but it is not applicable to information. If the legal doctrine of possession is extended to include knowledge of information, one cannot be divested of that form of possession, absent some form of induced amnesia. This then presents problems for those who, having come into possession of information, then wish to divest themselves of that possession: one can have a change of heart with cocaine and flush it down the toilet; one cannot put up one's hands and claim 'I'm no longer in possession of that knowledge'. There will always remain the argument of residual memory.

75 There is also an element of mens rea related to the possession of the information. What this might be is discussed below.

76 While possession can be jointly held, all joint possessors can be dispossessed by the act of one person who assumes exclusive control.

There are also problems with the way in which the actus reus of physical control and the mens rea of knowledge run together. The law on physical possession seems to establish that once a person knowingly takes control of an item it remains in their possession even if that person then forgets about it.[77] This is of benefit to those wishing to claim possession of lost rings,[78] but detrimental to those wishing to claim ignorance of child pornography or drugs.[79] However, if what is being 'possessed' is information, knowledge of that information constitutes both the act of control and also the mental element of knowing. So it would seem that those who are told a password but then later claim to have forgotten it could arguably still be in possession of the password because they might remember it later. Clough argues that for criminal law, this offends against the principle of coincidence between actus reus and mens rea.[80] He reasons that:

> If, and it may be a big 'if', the jury accepts that the defendant was no longer aware that it was in his or her custody or control, then the defendant is not in possession at that time. To treat the defendant's former knowledge as having somehow continued, despite evidence to the contrary, offends against the fundamental principle that the external and fault elements of an offence must exist at the same time. It also imposes an objective fault element as the defendant's earlier state of mind is effectively deemed to continue until such time as he or she disposes of the item, irrespective of the actual subjective mental state of the defendant.[81]

1 *Possession of Information in Insider Trading Offences*

This is not the first set of Australian offences to refer to possession of information. Insider trading law, also features possession of information as an element of the offence. However, this use of possession in relation to information occurs in a very different legislative context to that surrounding the identity crime provisions. The main offence is:

> **1043A Prohibited conduct by person in possession of inside information**
>
> (1) Subject to this Subdivision, if:
>
> (a) a person (the insider) possesses inside information; and
>
> (b) the insider knows, or ought reasonably to know, that the matters specified in paragraphs (a) and (b) of the definition of inside information in section 1042A are satisfied in relation to the information;

77 *Police v Kennedy* (1998) 71 SASR 175.

78 See *Parker v British Airways Board* [1982] 1 QB 1004.

79 See, eg, *R v Dib* (1991) 52 A Crim R 64; *R v Micallef* (2002) 136 A Crim R 127; *Police v Kennedy* (1998) 71 SASR 175.

80 In practice, the coincidence issue may be partly avoided. While the drug user has flushed the cocaine down the toilet and pornography viewer has deleted the image file, both can both still be charged with possession at a time prior to arrest, though this is a practice that contains its own issues. Forensically, prior possession is not as easy to prove as possession at time of arrest, and there are also issues with the availability of search warrants if there is no current possession. There is also an advantage in being able to show remorse or desistance in the criminal activity as part of any argument for mitigation of sentence. From a theoretical and principle perspective, the objection to a crime that creates an inability to repent is strong.

81 Jonathan Clough, 'Now You See It, Now You Don't: Digital Images and the Meaning of "Possession"' (2008) 19 *Criminal Law Forum* 205, 226.

> the insider must not (whether as principal or agent):
>
> (c) apply for, acquire, or dispose of, relevant Division 3 financial products, or enter into an agreement to apply for, acquire, or dispose of, relevant Division 3 financial products; or
>
> (d) procure another person to apply for, acquire, or dispose of, relevant Division 3 financial products, or enter into an agreement to apply for, acquire, or dispose of, relevant Division 3 financial products.[82]

Under these provisions, it is not a crime to possess insider information. Instead, criminality is based on dealing in shares to which the information is relevant, where the person ought to know the information is inside information. It is not a crime to possess the information, nor is it a crime to intend to engage in insider trading. In order for the offence to crystallise, one must engage in the criminal act of trading, with the mental element of knowledge of the information. The offence thus requires an overt act and in that sense is similar to the financial information offences.[83]

Discussion of the concept of possession of information in insider trading cases may shed some light on how the courts will interpret this aspect of the identity crime provisions.[84] The insider trading cases acknowledge that possession in this context does not mean possession in the property sense of physical control and intention to control, but instead refers to an awareness of the information.[85] This is in contrast to the 'lost property' and drug possession cases mentioned above which permit a notion of constructive knowledge in establishing possession. If direct personal knowledge is required for 'possession' of the narrowly defined 'insider information', there is a much stronger argument for such a requirement of liability under the far broader scope of information that can be prohibited under the identity offences. 'Possession' in this context thus approaches a synonym for knowledge.

These considerations also suggest that possession of information in an identity theft offence would require the accused to be aware of the nature of the information as 'identification information' – rather than another type of information. This seems clear from the line of High Court authority on the meaning of possession in drugs offences arising out of *He Kaw Teh v The Queen*.[86] In applying *He Kaw Teh*, the High Court in *Saad v The Queen* has held:

> In a case such as the present where it is necessary to show an intention on the part of an accused to have in his possession a narcotic drug, that intent is established if the accused knew or was aware that an article which was intentionally in his possession comprised or contained a narcotic drug. That is not to say that actual knowledge or awareness is an essential element of the guilty mind required for the commission of the offence. It is only to say that knowledge or awareness is

82 *Corporations Act 2001* (Cth) s 1043A.

83 See, eg, *Criminal Code Act 1995* (Cth) s 480.4, discussed above.

84 The following paragraphs are based on an earlier submission in relation to the NSW legislation: Alex Steel, Submission on Crimes Amendment (Fraud and Forgery) Bill 2009 (Consultation Draft), Parliament of NSW, 2009.

85 See, eg, *R v Hannes* (2000) 158 FLR 359, [224] ff.

86 (1985) 157 CLR 523.

> relevant to the existence of the necessary intent. Belief, falling short of actual knowledge, that the article comprised or contained a narcotic drug would obviously sustain an inference of intention. So also would proof of the possession of the forbidden drug in circumstances where it appears beyond reasonable doubt that the accused was aware of the likelihood, in the sense that there was a significant or real chance, that his conduct involved that act and he nevertheless persisted in that conduct. [87]

The passage makes clear that the intention to possess an item of a particular type requires an awareness that it is likely the item is of that type. Applying this approach to identification information an accused would need to know or believe that the information was identification information, or be aware that this was likely. This is the interpretation of possession adopted in the Victorian offences. These offences specifically include a requirement that the accused 'is aware that, or aware that there is a substantial risk that, the information is identification information'.[88]

Applying this to the identity crime offences in other Australian jurisdictions, it would seem an accused must be aware that the information in question is likely to be able to be used to identify persons – though not what the specific information entailed – before a conviction could lie.[89] This is of particular relevance if the information is held in a physical form that has not been read by the accused.

Together these factors create significant complexity. Consider the following scenarios. The accused is told:

a) that person's name is John Smith. That's what you should put on the false passport;

b) this letter contains that person's home address. You can use that to make the false passport; and

c) keep this envelope for James so he can make the false passport – the envelope is sealed and blank.

In scenario a) the accused knows the identification information. In scenarios b) and c) the accused has physical possession of a document containing information, but does not know what that information is, and in c) is not aware that it is identification information. It would also be difficult to establish in c) that the accused was aware the information was likely to be identification information. Applying the approach in insider trading cases – that one must have some awareness of the information – it may well be that scenarios b) and c) do not amount to possession of information. Similar issues arise if the information is in an encrypted digital form.

---

87 (1987) 70 ALR 667, 668.

88 *Crimes Act 1958* (Vic) ss 192B(1)(a), 192C(1)(a).

89 There would not be a requirement that the accused know the legal consequence of that categorisation: *R v Turnbull* (1943) 44 SR (NSW) 108, 109. That is, the accused would not need to know it was identification information as defined in the legislation.

2 *Comparisons with Digital Child Pornography Offences*

A comparison with the law on possession of digital child pornography illustrates the practical implications of possession as an element of identity crime. The child pornography offences also rely on an extended concept of possession, in this case covering digital files of images. The child pornography cases establish that a person is not in possession of data if all that exists on the computer are parts of files that cannot be retrieved or viewed by the person.[90] This is because the degree of control required must amount to an ability to view the image. Further, the digital pornography cases have made clear that the mental requirement of possession is one of an intention to control the item and that possession cannot be established if the person knows of the file on their computer but believes it is inaccessible.[91]

This again raises the question of whether a person in control of encrypted identification information, where the data was encrypted by another, is in possession of that information. Although the person physically controls the information, it is in an unreadable form, and in these circumstances the person is also unlikely to be aware of the detail of the information. The pornography cases would suggest that there is no possession of this information. This is particularly pertinent for the prosecution of data mules – people, often young travellers, who carry data files across jurisdictions but with no knowledge of what information is contained therein.[92]

On the other hand, if the data is readable but not read (as in a letter in a sealed envelope), Canadian decisions on pornography offences have held that this amounts to possession.[93] The case law relates to situations in which a person intentionally downloads a file, but deletes it without viewing the image. This is presumably by analogy with the doctrine of constructive possession of tangible items in containers, or property on enclosed land. One key aspect of this reasoning appears to be that the accused has a belief as to the content of the file. In the examples above, this case law is analogous to scenario b), where the accused is told of the content of the letter.

Similar issues arise with the situation in scenario c). It seems unjust to determine the conviction or acquittal of a data mule on the basis of whether the data carried is encrypted. This suggests that liability will turn then, not only on a question of whether the information can be accessed, but also on what the accused's belief is, if any, in relation to the material containing the information.

---

90 *Clark v The Queen* (2008) 185 A Crim R 1; *R v Porter* [2006] 1 WLR 2633, 2639.

91 *Littlejohn v Hamilton* [2010] TASSC 4. The example given is where a person deletes a file in such a way that they believe that they cannot retrieve it, but also believe that law enforcement might be able to using specialist software.

92 Cf Nicholas Cowdery, 'Use of Mules to Commit Fraud and Launder Money' (Paper presented at Pacific Fraud Summit 2007, 19 March 2007).

93 *R v Daniels* (2005) 191 CCC (3d) 393, 397 (Welsh JA), upheld in *R v Morelli* [2010] 1 SCR 253.

3 *Implications of the Two Approaches*

The line of reasoning in the child pornography cases makes clear that the ability to rely on notions of constructive possession really turns on the fact that the so called information is held in a physical or digital form separate from the mind of the accused. In such circumstances what is actually being prohibited is the possession of data, not information.

When this approach is contrasted with the approach in the insider trading cases it becomes apparent that while the child pornography cases concentrate on data – which in an electronic context is stored physically and can be constructively possessed through possession or control of the hard drives in which it is stored – information itself is something that resists these property analogies and must be actually known. That is, the information must enter the memory of the accused before possession will arise.

For all of these reasons it is argued that possession is an unfortunate basis on which to base liability for knowledge.

4 *The Canadian Approach:* R v Morelli

The above analysis has been confirmed in the recent Canadian Supreme Court decision of *R v Morelli* ('*Morelli*').[94] The decision is significant in that it is the first time digital possession has been considered in a nation's highest court. In *Morelli* the accused had viewed child pornography on his computer but had not saved the image files to his hard drive. The Canadian Criminal Code has separate offences for 'accessing'[95] and 'possessing'[96] pornography. A question for the Supreme Court was whether the viewing of a pornographic image on the screen, which led to an automatic saving of the file in the computer's cache, meant the accused was in possession of the file, or whether the image was merely accessed.

The majority held that viewing files in an internet browser amounted to accessing, but not possessing, that image.[97] In so finding, the Court's reasoning maintained a strong link with the traditional meaning of possession. Justice Fish (McLachlin CJ and Binnie and Abella JJ agreeing) noted that the law of possession had 'developed in relation to physical, concrete objects. Its extension to virtual objects ... presents conceptual problems'.[98] The majority held that possession in this area could be based on either 'the image file [or] its decoded visual representation on-screen'.[99] The judgment went on to note that Canadian case law supported a requirement that possession be of the underlying image file and agreed, stating:

---

94 [2010] 1 SCR 253.

95 *Criminal Code*, RSC 1985, c C-46, s 163.1(4.2).

96 *Criminal Code*, RSC 1985, c C-46, s 163.1(4).

97 The dissenting judgment of Deschamps J (Charron and Rothstein JJ agreeing) agreed that knowing control was central to possession, but disagreed that an act of intentional downloading of the file was the only way to prove possession: *Morelli* [2010] 1 SCR 253, [137]–[145].

98 *Morelli* [2010] 1 SCR 253, [18].

99 Ibid [19].

> [28] Interpreting possession to apply only to the underlying data file is also more faithful to a traditional understanding of what it means to 'possess' something. The traditional objects of criminal possession – for example, contraband, drugs, and illegal weapons – are all things that could, potentially at least, be transferred to another person.
>
> [29] Without storing the underlying data, however, an image on a screen cannot be transferred. The mere possibility of sharing a *link* to a Web site or enlarging the visual depiction of a Web site, as one could 'zoom in' on a TV screen image, is insufficient to constitute control over the content of that site. It is indeed the underlying data file that is the stable "object" that can be transferred, stored, and, indeed, possessed. More broadly, the object possessed must itself have some sort of permanence.
>
> [30] Thus, while it does not matter for the purposes of criminal possession how briefly one is in possession of the object, the thing said to be culpably possessed cannot – like a broadcast image flickering across a TV screen or a digital image displayed transiently on-screen – be essentially evanescent.
>
> [31] Plainly, the mere fact that an image has been accessed by or displayed in a Web browser does not, without more, constitute possession of that image.

The majority further held that a computer's automatic caching of files when viewing an image did not of itself constitute evidence of possession, because the mens rea of possession required intention to control and many computer users were unaware of the caching system.[100]

The decision is relevant in a number of respects. First, it reaffirms the argument above that possession is tied to property concepts, and emphasises that possession requires identification of an item that has some permanence. This suggests that something as evanescent as information should not be described using concepts of possession. Secondly, it rejects a reductionist approach to possession that would permit even momentary manipulation of images as control sufficient to amount to possession. This reasoning, if applied to the information offences, suggests there is a need to demonstrate that the accused is fully aware of the information and has made steps to acquire it. Possession in the information context is likely to require evidence that the accused either knew all of the relevant information or had an opportunity to find out and chose to not do so.

The decision also suggests that there is a distinction to be drawn in digital pornography offences between 'seeing' and 'keeping'. If this were applied to information offences, it could be that hearing or reading information would of itself not amount to possession. What might be required would be an attempt to memorise the information or to reduce it to some permanent format.

5 *Possession of Information: Is There Really a Problem?*

For the sake of completeness there is one final point to be made. An apparently simple and convenient solution to these doctrinal difficulties is simply to see the use of possession in these offences as a new way of using the term that is specific to this particular information and not linked to tangible property – contrary to the approach taken in relation to child pornography offences.

100 Ibid [36]–[37].

There are two objections to this proposition.[101] The first is that it would mean that accused, law enforcement and courts alike would be faced with a fundamental term that was sui generis and without any historical analytical framework within which to define it. This goes against the grain of the development of common law interpretation, which relies heavily on elaboration by analogy and attempts to treat like concepts as equally as possible.

The second objection can be described as the Humpty Dumpty objection. In *Through the Looking-Glass and What Alice Found There* by Lewis Carroll, Humpty Dumpty confounds Alice by insisting that 'glory' means 'a nice knock-down argument'. Carroll writes:

> When *I* use a word, Humpty Dumpty said, in rather a scornful tone, it means just what I choose it to mean – neither more nor less.
>
> The question is, said Alice, whether you *can* make words mean so many different things.[102]

A fundamental rule of communication is that words should have a shared common meaning, rather than mean different things to different people, or in different contexts. Possession as understood by the law is already a complex concept under stress in a number of areas, such as its applicability to digital forms of property and in relation to minute quantities. The rule of law requires that as far as possible legal terms should have a single meaning. It becomes necessary then to properly define the nature of the activity prohibited in identity crime and avoid the imprecise use of a largely incompatible term based on definitions of tangible property.

D Dealing in Identification Information

The flawed basis of the possession offences also affects the interpretation of the more serious 'dealing offences'. These make it an offence to:

- '[make, supply or use] identification information with the intention of committing, or of facilitating the commission of, an indictable offence' (NSW; Western Australia);[103]
- 'makes, supplies or uses identification information ... [and] intends to use or supply the information to commit an indictable offence, or facilitate the commission of, an indictable offence' (Victoria);[104]
- '[make, supply or use] identification information [with an intention that] any person ... will use the identification information to pretend to be, or

101 These objections apply to the insider trading offences as well. However, in those offences, the 'possession' of the information is not in itself an offence and so the difficulty is less critical as, irrespective of the meaning of the term, liability rests on a deliberate activity of trading.

102 Lewis Carroll, Martin Gardner and John Tenniel, *The Annotated Alice: Alice's Adventures in Wonderland and through the Looking Glass* (Penguin, 1970) 269.

103 *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009* (NSW) s 192J; *Criminal Code Amendment (Identity Crime) Act 2010* (WA) will insert a new section 490 into the *Criminal Code Act Compilation Act 1913* (WA). The WA offence uses 'material' instead of 'information'.

104 *Crimes Amendment (Identity Crime) Act 2009* (Vic) s 192B.

to pass the user off as, another person ... for the purpose of ... committing [or facilitating] an [indictable] offence' (Commonwealth);[105]

- Deal [including supply or use] in identification information with 'the purpose of committing, or facilitating the commission of, an indictable offence' (Queensland);[106] and
- 'Make use of another person's personal identification information intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence' (South Australia).[107]

These offences replicate the mental elements of the possession offences and, other than in Queensland, provide much higher maximum penalties than the dealing offences. But, penalties aside, the only difference to the drug possession offences is the 'use'[108] of the identification information. And again there is no description of the prescribed uses of the information, and so potentially any 'use' is prohibited. The breadth of the offences in all jurisdictions other than the Commonwealth means that behaviour that extends well beyond fraud or theft is nonetheless captured by the provisions. As the information can be used with the consent of the person it identifies, there is no requirement that the identification information be used dishonestly. Thus it is now an identity crime in NSW for a tax agent to submit a false tax return (itself an offence), even if the client concurs. In such cases there is no intention to deceive in relation to the person's identity, quite the opposite. The breadth of these laws criminalises conduct that is an ancillary but necessary part of another crime, but which in itself was not hitherto unlawful. In the example just described, tax fraud and conspiracy offences have been committed, but – by conventional standards at least – not an identity crime.

This is an inappropriate basis for criminalisation. If this basis were acceptable, similar crimes of using a car, a phone, an umbrella, or a torch to facilitate the commission of a crime could be justified. Any arbitrary additional element could be criminalised: types of clothes worn, days of the week, or anything else.

Liability should instead be based on a combination of activities and circumstances combined with mental elements. There needs to be a clear explanation of why the additional element amounts to an added or different form of criminality that requires specific prohibition. (For example, a use of violence when stealing causes a risk of harm to the victim and so justifies the additional criminality of robbery. The type of violence committed and the weapon used also provides a range of justifications for differential penalties.)

105 Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 (Cth) sch 1 pt 1 cl 372.1.

106 *Criminal Code Act 1899* (Qld) s 408D(1).

107 *Criminal Law Consolidation Act 1935* (SA) s 144C.

108 Supply would seem to be a subset of use, and it is difficult to see how one 'makes' information. Presumably this means the creation of false identities.

In the proposed Commonwealth version of this offence, the end result is specified: that of impersonating another. This at first glance appears a much more acceptable basis for criminalisation than the state and territory approaches to identity crime. The Commonwealth provision makes clear that the identity offence is an ancillary and preparatory offence linked to fraud offences. While this expansion of the law might be criticised, at least the conduct at which the offence is aimed is apparent. Having said this, the Commonwealth offence creates a more extenuated version of the offence than do the State offences, in that the accused need not be the person facilitating the crime by either using or supplying the information.

V SOME OTHER DISTURBING ELEMENTS OF THE IDENTITY THEFT OFFENCES

A Non-Manifest, Non-Act Crimes

These offences are crimes of non-manifest criminality. George Fletcher famously argued that many crimes could be seen to exist on a spectrum, with manifest criminality at one end and non-manifest or subjective criminality at the other. Crimes of manifest criminality are those that are objectively discernable at the time they occur, such as when a person is caught red handed in a burglary.[109] At the other end of the spectrum are crimes where there is nothing in the prohibited acts that would allow a bystander to identify the behaviour as a crime.[110]

Possession of information is an offence at the extreme end of non-manifest criminality. The criminality lies entirely in the mental elements of the crime. It is not unlawful to possess any of this information, the crime is entirely in the intention with which the information is possessed. Indeed, there is no act at all in possession, it is a continuing status.[111]

This raises real problems of proof. If a person is found with the credit card numbers of others, prosecutors will need to rely on a confession or inferences to obtain a conviction. They cannot point to anything the accused has done as indicating criminality. If there is no confession, conviction will be based almost entirely on inferences and assumptions – many of which may amount to assumptions of guilt in the absence of alternatives being put by the defence.

The problems of proof have been explicitly acknowledged in Western Australia by the Attorney-General:

> But I will say it again, so that it is on the record for the purposes of this bill, and in case this debate is ever looked at for the purpose of interpretation, that the problem sought to be cured by this bill is the fact that it would be very difficult to prove an attempt to an offence in a circumstance in which a person was in

109 Fletcher, above n 72, 116.

110 Ibid 233.

111 As discussed above, the acts relevant to possession are the prior taking of possession, and the future disposal of possession – neither of which fall within the elements of the crime.

> possession of material that was otherwise innocuous. … Under this legislation, if we could get across the hurdle of proving the intent to commit an offence, the fact that a person was in possession of another person's identification material or information would give rise to at least the possibility that there would be an appropriate offence for which to prosecute that person. [112]

What is deeply concerning in these circumstances is the artificial solidifying of the alleged intent. The nature of any mental attitudes a person has to certain events is likely to change over time. As well, one may be unclear as to one's own mental state. As Larry Alexander and Kimberly Ferzan have noted, when a person wishes their mother-in-law dead, it is uncertain whether this is an intention (hopefully unfulfilled) or merely a desire or wish.[113] Questions from law enforcement could lead a person to admit to a firm intention that was not in fact that person's dominant state of mind. Similarly, a person with identification information belonging to a rival may be motivated to wreak revenge on that rival, but that intention alone may not be strong enough to actually lead the would be avenger to take any action. Yet this would seem to be enough to render this person guilty of identity theft offences; especially if they made unwise admissions, or were found in apparently incriminating circumstances.

The situation becomes further complicated in the case of a person who has a conditional intention. Take for example the passing thought, 'I will use this information to commit identity fraud if I am retrenched'. Given the situation of retrenchment has not yet occurred, and may never occur, is this intention sufficient to justify criminality?[114]

Legislative and common law definitions of intention are of no real assistance here. Thus the Commonwealth *Criminal Code* defines intent to be that the person 'means' for the event to occur[115] – merely inserting a dictionary synonym for intention.[116] Queensland uses the term purpose instead of intention, but does not go on to define it. The common law defines intention variously,[117] but judges are advised to not define the term for jurors: apparently it is a commonsense term that juries will intuitively understand.[118] The main reason for this approach is that overwhelmingly intention is only considered following the commission of an act (*actus reus non facit mens rea*) and is assessed in relation to that act.

Indeed, the common law refused to allow such non-act situations to amount to crimes. It was held in *R v Heath* in 1810 that: '"having in his possession" with

---

112 Western Australia, *Parliamentary Debates*, Legislative Assembly, 19 November 2009, 9475–6 (Christian Porter, Attorney-General).

113 Larry Alexander and Kimberley Ferzan, *Crime and Culpability* (Cambridge University Press, 2009) 202. The discussion is based on a quote from Gerald Dworkin and David Blumenfeld, 'Punishment for Intentions' (1966) 75 *Mind* 396, 401.

114 Alexander and Ferzan, above n 113, 199–216.

115 *Criminal Code Act 1995* (Cth) s 5.2.

116 Ian D Leader Elliot, *The Commonwealth Criminal Code: A Guide for Practitioners* (Commonwealth Attorney-General's Department, 2002) 53.

117 See Simon Bronitt and Bernadette McSherry, *Principles of Criminal Law* (Thomson Reuters, 3rd ed 2010) 199–203.

118 Judicial Commission of NSW, *Criminal Trials Bench Book* (18 May 2010) [3-210] <http://www.judcom.nsw.gov.au/publications/benchbks/criminal/intention.html>.

the terms knowingly, &c. annexed to it could not be considered an act, and that an intent without an act was not a misdemeanour.'[119]

It is for these reasons that inchoate offences such as attempt require some act to be undertaken. Committing an act demonstrates the firmness and solidification of intention into something that attracts liability. Even then, the person who desists at an early enough stage may yet escape liability.[120] This safeguard – requiring some firmly demonstrated intention – does not form part of the information possession offences.

Further, the 'dealing in information' offence – which proscribes an act and thereby mirrors the structure of attempt offences – does not contain any mechanism for assessing whether the nature of the use or supply of information is sufficiently connected to the crime, nor whether it advances its commission sufficiently to warrant culpability. The distinction between preparatory acts and acts of perpetration remains a vexed one in the law of attempt, failing to provide any clear definition between the two, but the essential concept is clear.[121] This was considered an important limit to the criminal law by the drafters of the *Model Criminal Code* when they concluded that liability should only arise in the instance of attempt when the act had become one of perpetration and not merely preparation and an act that was only a substantial step towards commission of the crime was an insufficient basis for liability.[122]

The failure in all jurisdictions other than the Commonwealth to limit the crime intended to be committed with the identification information to a specific type of indictable offence also compounds the problem of over-criminalisation. Indictable offences are not only contained in *Crimes Acts* or *Criminal Codes*. There is also an increasing multitude of indictable offences in legislation that regulates areas of generally legal activity. While such regulatory legislation is largely civil in nature, breaches of the regulatory scheme are often defined as crimes. This has the effect of potentially increasing the penalty of much behaviour in business.[123] Further, on the face of the NSW legislation, there is no requirement that the information is intended to be used in the commission of the crime.[124] This surely must be an ellipsis, for otherwise every offence would also be an identity crime as everyone has knowledge of information relevant to the identity of others. But even if there is a need to prove an intention to use the information in connection with a proposed crime, there arises the question as to the specificity with which prosecutors will need to allege the exact crime intended. If the courts accept that the inchoate nature of the offence is such that

119 See *R v Heath* (1810) Russ & Ry 184.

120 See, eg, *R v Susak* (1999) 105 A Crim R 592; cf *Page* [1933] VLR 351.

121 Cf *DPP v Stonehouse* [1978] AC 55.

122 Standing Committee of the Attorneys-General Model Criminal Law Officers Committee, *Final Report on General Principles of Criminal Responsibility* (1992) 77.

123 See Uniform Legislation and Statutes Review Committee, Parliament of Western Australia, *Report 44: Report on Criminal Code Amendment (Identity Crime) Bill 2009* (2010) 38–45.

124 *Crimes Act 1900* (NSW) s 192J.

the intended crime need only be of a particular type,[125] the potential for the use of the offence as a broad sweep offence is high.

What is also unclear in these offences is the *degree* of awareness of the particular crime to be committed. If, as is likely, the courts see these offences as inchoate offences similar to attempt and accessory before the fact, the High Court's requirements in *Giorgianni v The Queen* will apply.[126] That is, the person must know of all the 'essential facts' of the alleged consequent offence and intend that all those facts to occur.[127] This will presumably require proof of a detailed briefing or evidence of planning in relation to the proposed crime. It is unlikely that data mules would have such knowledge, and in fact would most likely be deliberately kept ignorant of the end aim. The result may then well be that those most directly involved in the organised criminal trafficking of personal information will be the only people immune from prosecution.

More fundamentally, the move towards basing liability on the mental state, rather than the actions, of the accused represents a move towards a legal system that 'make[s] criminal dangerous persons rather than dangerous conduct'.[128] Given the extreme breadth of these offences, there are questions over whether the new laws make the majority of the population prima facie dangerous.

B Measuring Criminality by Penalty

A further worrying aspect of the new legislation is that it is said to be part of a national scheme and yet it remains inconsistent across jurisdictions. The differences in wording have been discussed above. What is of more concern is that there are significant differences in maximum penalties across jurisdictions. Maximum penalties are generally seen by the public as reflecting the seriousness of the crime and are taken into account by courts as a yardstick for setting the correct penalty.[129] The differences across Australia are set out below:

Table 1: Maximum penalties (imprisonment by years)

Jurisdiction and year enacted	SA (2003)	Qld (2007)	Model Code (2008)	Cth (Bill 2008)	Vic (2009)	NSW (2009)	WA (2010)
Possess Identification Information	3	3	3	5	3	7	5
Deal in Identification Information	3	3	5	5	5	10	7

125 Cf attempt: *R v Bainbridge* [1960] 1 QB 129.
126 (1985) 156 CLR 473.
127 Ibid 502–3.
128 Norman Abrams, 'The New Ancillary Offences' (1989) 1 *Criminal Law Forum* 1, 35.
129 *Markarian v The Queen* (2005) 228 CLR 357, 372.

What emerges here is that not one jurisdiction has adopted the penalty scheme of the Model Criminal Code. There has been an overall increase in maximum penalties over time and NSW has by far the most punitive regime. Identity crime is a national and international crime, rather than one that is likely to occur with different intensities and in different guises in local areas. Given this, there is no justification for such a disparity between maximum sentences. It strongly suggests that the setting of penalties is based on local political factors rather than any reasoned national approach. As such, it brings into question any claims that there is a shared national understanding of the seriousness of these activities.

As we have seen, the breadth of activities caught by the offences is extraordinarily wide. In such circumstances it is troubling that NSW feels a maximum penalty of up to 10 years is warranted for such preparatory behaviour.

C Moving the Locus to Law Enforcement

There are now increasingly few transactions in modern life that can be completed without providing personal details. Offences of the breadth of the identity crime provisions have the effect of creating significant scope for 'back-up' offences that criminalise aspects of behaviour that do not warrant any or additional sanction.[130] Failure to define such offences in a limited way means that inevitably police and prosecutors are expected to exercise discretion as to which instances to prosecute. This then has the effect of moving the locus of defining criminality away from the legislature and onto law enforcement.[131] This leads to a diminution of the rule of law;[132] that is, there is a decrease in the degree to which it can be predicted that certain punishments or consequences will flow from certain actions. Instead, the extreme breadth of the offences require selective enforcement and wide discretion in charging on the part of law enforcement officers. There is little doubt that such laws are more in the mould of discretionary police powers than uniformly enforced offences. As the NSW Attorney-General stated in the second reading speech introducing the NSW provisions:

> It will now be a very serious crime, punishable by up to 10 years imprisonment, if a person deals in identification information. This will include using it, making it or selling it. It is a growth crime, costing Australians millions of dollars a year and we are determined to *give police the power* they need to investigate and prosecute it.[133]

130 See, eg, Markus Dirk Dubber, 'Policing Possession: The War on Crime and the End of Criminal Law' (2001) 91 *Journal of Criminal Law & Criminology* 829; Douglas Husak, *Overcriminalisation: The Limits of the Criminal Law* (Oxford University Press, 2008), 27–31.

131 Abrams, above n 128.

132 Rule of law in a criminal context is expressed by the Latin phrase *nulla poena sine lege* (no penalty without law). For a detailed discussion of this diminution of rule of law, see Husak, above n 130, 27–31.

133 NSW, *Parliamentary Debates*, Legislative Council, 12 November 2009, 19507 (John Hatzistergos, Attorney-General) (emphasis added).

As discussed, these offences prohibit an exceptionally wide range of activity. In many cases, prosecutions are only viable if the accused has in fact already committed further acts for which liability arises. In such cases the identity offences will be back-up charges, or charges for which a plea of guilty can be an outcome down to which an accused has been negotiated. Laws such as these have been described by William Stuntz in the US context in the following terms:

> ... for the most part, criminal law and the law of sentencing define prosecutors' options, not litigation outcomes. They … are items on a menu from which the prosecutor may order as she wishes. She has no incentive to order the biggest meal possible. Instead, her incentive is to get whatever meal she wants, as long as the menu offers it. The menu does not define the meal; the diner does. The law-on-the-street – the law that determines who goes to prison and for how long – is chiefly written by prosecutors, not by legislators or judges.
>
> The bodies of law … that claim to define crimes and sentences do not really do what they claim. Instead, those bodies of law define a menu – a set of options law enforcers may exercise, or a list of threats prosecutors may use to induce the plea bargains they want. The menu says little about what options are exercised or what threats are used. The real law of crimes and sentences is the sum of those prosecutorial choices. *That* law is nearly opaque; even those who study the criminal justice system for a living know very little about it.[134]

Longer term, the enactment of these offences is likely to bias prosecutors towards charging these easier to prove offences, rather than the substantive offences they are designed to complement. This can then lead to an impoverishment of the substantive criminal law, with the main offences subordinated to these fringe offences.[135]

VIII CONCLUSION

It is undeniable that identity crimes are a significant and growing problem for law enforcement. The true extent of internet related identity crime remains unclear, and as a result the fear of its effects remains significant. Fundamental aspects of the internet and electronic commerce make law enforcement via traditional means highly problematic.

The confluence of these issues has led most Australian legislatures to enact sweeping information possession offences. However, these offences are unacceptably broad and vague. First, they centre on knowledge of information that in most cases is publicly available and legal to acquire: the offences turn an otherwise lawful situation into a serious crime based entirely on the ulterior intention of the accused to use this information in relation to an indictable offence. There is no requirement that the intended crime hinge on this information for its commission, and it remains unclear what degree of connection the information must have to the intended ulterior crime. It seems possible that

134 William J Stuntz, 'Plea Bargaining and Criminal Law's Disappearing Shadow' (2003) 117 *Harvard Law Review* 2548, 2549, 2569.

135 See the discussion in Abrams, above n 128, 32–5.

the information may be used as part of an activity that of itself is entirely lawful. In this regard the Commonwealth Bill offence is preferred to the offence in other jurisdictions, in that it requires that the information be used to create a false identity as part of an indictable offence. This focuses the offence on fraud facilitation and so prevents the identification offence becoming a broad back up offence for a very wide range of crimes.

There are also fundamental problems with reliance on the notion of ulterior intention alone to establish criminality. Generally, inchoate offences require proof of some overt act to establish that the intention is sufficiently firm to justify criminal liability. By contrast, the identity offences do not require any such degree of solidity in the intention. Given that an accused is likely to deny the intention existed, there exist concerns about the possible over reading of circumstantial evidence.

Not only is the scope of these offences overly broad, but the doctrinal basis is inappropriate. The offences are based around a concept of possession of information. The legal meaning of possession is highly complex and historically based around tangible personal property. Courts have acknowledged that there are conceptual difficulties with extending possession to cover digital computer files. These difficulties can however be accommodated to a large extent because of the physical location in time and space of such files, and their recognition as discrete items of property. Neither of these constraints easily apply to information. Fundamentally, the fact that information is not recognised as property means that it is not possible to use possession in its general property law sense, and the danger of a Humpty Dumpty approach to law arises. As the Canadian Supreme Court's recent analysis of digital pornography shows, possession is useful as a way of differentiating momentary or evanescent access to something from a more permanent acquisition. This important distinction is difficult to draw with information acquisition if it labours under the forced label of possession.

This paper has argued that if it is desirable to prohibit such preliminary steps in identity fraud offences, legislatures should define the activities that are to be prohibited – that is, the acquisition and distribution of such information in material or electronic forms. Unless it can be shown that the nature of the item possessed is inherently dangerous, the criminal law should eschew the use of status offences such as possession. No such case can be made for personal information without more.

The extreme breadth and lack of specificity of these offences shows a clear legislative intent to give police a wide degree of discretion. It allows police to charge those they suspect of planning to engage in serious criminality on the basis of otherwise innocuous and innocent behaviour. Such an approach might well appeal as a quick fix to law enforcement, but it is destructive of the underlying principles of a fair and just criminal law. Much more attention needs to be given to a systematic attempt to properly describe the activities that need to be prohibited to prevent identity crimes, and there is an urgent need for legislatures to provide a reasoned justification for criminalisation of such inchoate behaviour.