



IDENTITY CRIME

**Management of Serious Crime program
Australian Federal Police College, Barton**

2 October 2007

Bruce Arnold
www.caslon.com.au

Key Points

■ **diversity**

Identity crime in the digital era is diverse.

Just as in the past, identity crime (sometimes tagged as 'identity theft') involves a range of offences – some more serious than others – affecting all parts of the community. It is more than credit card fraud, welfare fraud or kids using photoshopped proof-of-age cards.

■ **responses**

Effective responses to identity crime require an agnostic, technology-neutral approach.

The diversity of identity crime and challenges in reporting and data analysis means that there are major uncertainties about most identity crime statistics. Consumer perceptions of threat and risk are often misplaced. Official responses may be inappropriate, driven by media releases and solution vendors rather than what empowers business, individuals and law enforcement personnel. Much 'digital' identity crime is low tech and involves family members, not the Vladivostok mafiya. Solutions such as the 'Australia Card Mark II' will reduce some identity offences but increase other identity crime.

■ **it's a people problem**

Identity crime in the digital era is about people, not about technology.

Digital technologies provide tools for enabling, inhibiting and identifying identity crime. ID crime is based on human nature and basic economics. We take things on faith, we believe what appears to be authoritative – a bit of paper, a persuasive claim, something on the net – and we don't verify some claims because that would involve costs and delays.

■ **a modern epidemic?**

Identity crime is not the "crime of the millennium", something that is out of control or about to become out of control.

Much contemporary identity crime is a creature of the media, rather than the internet. It does not require radical new legislation or special agencies. Perceptions of incidence, severity and demographics are influenced by how journalists report particular offences, how offences are conceptualised by law enforcement personnel and whether some information is identified by data custodians.

IDENTITY CRIME

■ introduction

“Crime of the century”?¹ As American as apple pie and the drive-by shooting? As Australian as mateship? Perpetrated by the Siberian mafiya? Or by the kid next door?

This paper for the Management of Serious Crime (MOSC) program of 2 October 2007 accompanies a presentation on ‘identity crime’ – a term that characterises a range of offences and practices.²

The paper covers –

- the nature of identity crime
- past and contemporary practice
- costs
- impacts and uncertainties
- identity crime law
- other responses
- some recent developments

■ the nature of identity crime

What is identity crime? The most useful answer to that question is probably that it is a way of thinking about identity-related offences rather than a specific crime, particularly a crime that it is new, unprecedented and primarily online.

Identity crime?

The notion of identity crime covers a wide range of offences, often dealt with through specific enactments and through common law (case law) that has evolved over the past 500 years. Some offences are very traditional, very low tech and small scale. Others are quite new and pose problems because they involve questions about identification, jurisdiction and so forth.

Some observers have argued that we should rely on terms such as fraud, identity theft, impersonation, forgery, credit card skimming, deception, cybercrime, ‘joe jobs’, health fraud and imposture.³

Others have suggested that there is value in bundling those offences or practices as ‘identity crime’, on the basis that they all involve questions of identity and that a particular offence (such as creation of a fake birth certificate or drivers licence) may

¹ *Locking Up The Evil Twin: A Summit on Identity Theft Solutions*, 2005 Californian government report at www.idtheftsummit.ca.gov/2005_report.pdf

² This briefing draws on a more detailed discussion of identity crime at www.caslon.com.au/idcrimeguide.htm and associated pages at www.caslon.com.au/datalossnote.htm.

³ Questions about terminology are highlighted in the 2004 *Standardisation of definitions of identity crime terms* from the Australasian Centre for Policing Research (ACPR) at www.acpr.gov.au.

be the basis for numerous other identity-related offences. One example is the recent *Identity Crime* discussion paper by the national and state/territory officials concerned with development of the model criminal code, highlighted below.

In essence, identity crime encompasses –

- appropriating someone else’s identity (eg forging a cheque, unauthorised use of another person’s credit card, unauthorised access to confidential data by pretending to be another person)
- using a fictitious identity
- massaging the offender’s own identity (eg deleting criminal convictions or financial misadventures from a CV, adding unentitled qualifications to a CV, amending a proof of identity document to gain a financial advantage or access to age-restricted premises).⁴

Identity crime occurs because most people do not live in a village: we deal with strangers and institutions on a daily basis and often rely on proofs of identity that range from whether someone is wearing a uniform or has a business card to whether the person can provide what appears to be an authentic drivers licence, credit card, passport or corporate security pass. Criminologists such as Gary Marx have wryly suggested that identity crime is one price we pay for not living in an environment where the nosy neighbours know everyone ... and know everything that is going on.

It also occurs because we want to believe or because we accept certain risks. In practice few people have much expertise in document forensics. The delays and other costs associated with comprehensive verification of identity are unacceptable for most commercial transactions and more broadly for much social interaction.

Who engages in identity crime?

If we look beyond the headlines about doctors who gained their surgical qualifications from a cereal packet and teams of rossiyskaya mafiya hackers exploiting millions of stolen credit card numbers we can see that different offences involve different types of people and affect business, law enforcement agencies and consumers in different ways.⁵

Your next contractor might be engaged in identity crime. So might one of your executives or a job applicant. Tonight several thousand kids will be using massaged proof of identity documents to gain entry to clubs. Some will be stealing ‘virtual gold’ (for the heck of it or conversion into real cash) by appropriating an avatar in a

⁴ The 2004 ACPR 2004 *Standardisation* discussion paper offered a broader set of definitions, problematically encompassing activities and possession of devices or tools. ACPR recommended use of ‘False Identity’ to describe creation of a fictitious identity, alteration of one’s own identity (identity manipulation) or theft or assumption of a pre-existing identity (identity theft). ‘Identity Crime’ was to be used as “the generic term” to include both identity fraud and identity theft (and ‘skimming’) and “relevant related offences (such as possession, distribution and manufacture of relevant items, devices etc)”. ‘Identity Fraud’ would denote the “gaining of money, goods, services, other benefits or the avoidance of obligations through the use of a false identity and should include instances of ‘skimming’”. ‘Identity Theft’ would describe “theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is alive or dead”.

⁵ See for example the 2007 *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement* by Gary Gordon, Donald Rebovich, Kyung-Seok Choo and Judith Gordon of the Utica College Center for Identity Management & Information Protection.

massive multiplayer online role-playing game.⁶ Other people will be collecting government benefits to which they are not entitled or using a blurred identity to evade obligations.

This paper does not purport to offer an in-depth exploration of identity crime. Instead, we can get some sense of the offences by highlighting particular historic and contemporary practice: what people have done in the past, what they are doing today.

■ past and contemporary practice

Identity crime predates the web, the credit card, the fax machine, the cheque and the steam engine. It occurs wherever people want to believe and have trouble verifying an identity.

If we look back in history we can thus see numerous incidents of identity crime –

- Isaac's fraud in *Genesis 27* (using Esau's robes, a bit of hair treatment and confirmation by Rebekah)
- medieval fraudsters who claimed to be Jesus Christ or, more modestly, a bishop or patriarch and usually ended up being boiled alive, burnt at the stake or impaled on a stick
- people who pretended to be a deceased or missing notable⁷, including over 30 imposters who claimed to be the son of Marie Antoinette⁸, several 'children' of the last Russian Tsar⁹ and the Wagga grocer who claimed to be Sir Roger Tichborne¹⁰
- scammers who persuaded victims that they had the authority to sell the Eiffel Tower, Brooklyn Bridge and other scrap metal.¹¹

The range of offences, and the variety of community responses, can be grasped by looking at some contemporary practice –

⁶ cf Edward Castronova's *Synthetic Worlds: The Business & Culture of Online Games* (Chicago: Uni of Chicago Press 2005), *The LAN Game Ate My Brain, Dude: 'MMORPG Addiction' and Australian Law* at www.caslson.com.au/publications/mmorpg2007.pdf and Julian Dibbell's *Play Money: Or, How I Quit My Day Job and Made Millions Trading Virtual Loot* (New York: Basic Books 2006).

⁷ One of the more entertaining instances was John of Powderham's 1318 claim that he and not the reigning Edward II should be king, explaining that a nurse had swapped babies after a pig had gnawed on his ear. He later retracted the claim, saying the Devil in the guise of a cat had inspired him. Both John and the cat were then hanged (rather unfair on the moggie); Edward was deposed in 1327.

⁸ One of the more implausible claimants was "tres noir", which raises questions about the credulity of his audience. Trauma in prison may have famously turned Marie Antoinette's hair white overnight but incarceration does not alter ethnicity.

⁹ The most famous example is the woman known as Anna Anderson; a slew of other pretenders have come forward and presented themselves as the children or grandchildren of Nicholas and Alexandra.

¹⁰ The Tichborne trial, discussed in Robyn Annear's *The Man Who Lost Himself: The Unbelievable Story of the Tichborne Claimant* (Melbourne: Text 2002), was for over 100 years the longest trial in England. Imposter Arthur Orton was eventually convicted of perjury and disappeared into obscurity; presumably these days he'd sell his rights to *Who Weekly* and feature in a mini series or in *Big Brother*.

¹¹ See for example Joseph 'Yellow Kid' Weil's memoir *Con Man: A Master Swindler's Own Story* (New York: Broadway 2004) and the biography of competitor 'Count' Victor Lustig in *The Man Who Sold the Eiffel Tower* (Garden City: Doubleday 1961) by Floyd Miller

Resume Fraud

Some identity crime involves people buffing their CVs, on occasion buffed out of recognition.

Some examples are –

- Ricardo Garotte stole £4 million from two UK banks after using false references to gain temporary employment
- Chris Tyler, CEO of Telstra subsidiary Solution 6, was revealed to have a drug conviction (with a ten year suspended sentence)
- Telstra colleague and former ANZ Bank CIO Bruno Sorrentino added a fake PhD to his CV
- John Friedrich, head of the Australian National Safety Council, concocted a CV in aid of a \$300 million scam
- Glen Oakley of the NSW Department of Business & Regional Development was revealed not to possess his BsC, MBA and PhD
- World Intellectual Property Organization Director General Kamil Idris reportedly added nine years to his CV, allegedly useful for early retirement
- a much-loved and apparently outstandingly efficient dean at MIT resigned after revelation that she didn't in fact possess the degrees that appeared on her resume
- IBM supremo Jeffrey Papows resigned after being savaged in the *Wall Street Journal* after embellishment of his CV¹²
- international terrorism expert Alexis Debat was revealed to have falsely claimed a PhD from the Sorbonne and to have concocted interviews with Kofi Annan, Alan Greenspan, Bill Gates and Michael Bloomberg
- 'Linda Astor' (aka 'Linda Hoffman') invented qualifications and referee Dr Zbigniew Poddubnick in gaining a job as Clinical Director of Mental Health in New Zealand.

How many dodgy CVs are in use? No one knows and many industry claims are problematical, because they conflate minor errors and omissions with significant falsification.¹³ Resume fraud has fed growth of the commercial vetting industry; unfortunately the effectiveness of much of that vetting appears to be poor.¹⁴ The

¹² In one of its more memorable putdowns *The Register* (30 April 1999) quipped that "So he's not an orphan, his parents are alive and well. He wasn't a Marine Corps captain, he was a lieutenant. He didn't save a buddy by throwing a live grenade out of a trench. He didn't burst an eardrum when ejecting from a Phantom F4, which didn't crash, not killing his co-pilot. He's not a tae kwon do black belt, and he doesn't have a PhD from Pepperdine University".

¹³ *Assessment Council News* in February 2003 noted a range of figures from 11% to 67%. It is common to encounter claims that "about one in four CVs contain lies", 500,000 fake degrees (with 10,000 fake medical degrees) are "in use" in the US, "75% of all CVs have some form of embellishment and 25% contain outright lies" and that 21% of applicants in the finance sector have engaged in "CV fraud", with around two thirds of that 21% omitting criminal convictions". The UK Chartered Institute of Personnel & Development claimed that one in four companies rescinded a job offer in 2004 because of CV fraud; 23% supposedly sacked staff after recruitment because of discrepancies. The figures should be viewed with caution: the most common offence appears to be exaggerating the applicant's current salary.

¹⁴ There is little case law on action by employers against executive recruitment or vetting agencies for failure to prevent such embarrassment. Presumably all parties simply want the problem to go away

adequacy of verification by some public and private sector entities poses liability concerns, with for example criticisms that health institutions in Australia and the US failed expectations of due diligence in checking the *vita* of Dr Jayant Patel and thereby allegedly contributed to the deaths of large numbers of patients.¹⁵

Some people don't bother with the CV.¹⁶ Barry Faulkner, for example, posed as a doctor at Royal Brisbane Hospital in conducting bogus examinations of pregnant women, before going to pose as a gynaecologist, member of The Monkees, CIA agent, Olympics official, pilot of sundry airlines, US Air Force colonel and Marine Corps captain.¹⁷

Christopher Rocancourt gained several million by pretending to be a Rockefeller heir, son of Sophia Loren, nephew of Dino De Laurentis and so forth. David Hampton, immortalised in John Guare's 1990 *Six Degrees of Separation*, gained attention during the 1980s in relieving wealthy Manhattanites of their money by convincing them he was Sidney Poitier's son.

Alan Conway – depicted in the 2006 film *Color Me Kubrick* – wined and dined his way through Europe in the guise of Stanley Kubrick. US waiter Abraham Abdullah picked up US\$20 million pretending to represent Warren Buffett, Oprah Winfrey and Steven Spielberg, persuading credit reference giant Experian and other gatekeepers to divulge information that facilitated his scam. When he was arrested he had a mere 800 fraudulent credit cards.

Stolen honour and appropriated sorrow

Some people, including those holding high profile positions in government and business, award themselves military honours. Appropriating honours, however offensive, may be a victimless crime: something that results in distaste or pity. However, it reflects badly on organizations that have been gulled.

James Montgomery, who had awarded himself a Victoria Cross (and claimed to have served as a US Marine, Australian SAS captain, SA major, commando and US Navy SEAL) was fired from Charles Sturt University in 2005. More recently we've seen the case of 'Colonel' Michael Nicholson, who used a fake ID to gain entry to Randwick Barracks (useful for free tailoring) and HMAS Watson.

'Major' Reg Newton claimed to be a secret agent, being awarded a Military Cross for acts of derring-do in Cold War East Germany and Mongolia. He was more modest than Captain Sir Alan McIlwraith CBE DSO MC: only the 'Alan McIlwraith appears to be authentic, despite his self-authored profile on Wikipedia and contrary to claims by some enthusiasts that wiki quality control is timely and effective.

rather than appear and reappear in the financial press or in lawsuits by aggrieved shareholders; some settlements may thus occur on a confidential basis.

¹⁵ The Patel (aka 'Dr Death') incidents are explored in the 2005 Bundaberg Hospital Commission of Inquiry ('Morris Inquiry'), Queensland Public Hospitals Commission of Inquiry ('Davies Inquiry') and Hedley Thomas' *Sick To Death* (St Leonards: Allen & Unwin 2007).

¹⁶ Frank Abagnale's experience, reported in *Catch Me If You Can* (New York: Broadway Books 2005) and consistent with the exploits of figures such as the 1906 'Hauptmann von Köpenick' and Virginia Woolf's 1910 impersonation of the Emperor of Abyssinia in a tour of *HMAS Dreadnought* suggest that a uniform and aplomb count for much.

¹⁷ US identity thief Ferdinand Demara assumed the identity of real or fictitious civil engineers, scientists, police, psychologists, lawyers, clergy and teachers. His career in crime peaked when he appropriated the identity of Canadian navy surgeon Joseph Cyr, supposedly successfully undertaking surgery during the Korean War.

More bizarrely, 22 year old sex offender Joshua Garner posed as the 17 year old Duke of Cleveland; 29 year old sex offender Neil Rodreick attended schools in Arizona and Oklahoma as a supposed 12 year old.¹⁸

Even more sadly, some people claim to be survivors of horrific events, whether for profit or simply to fill some personal need for love and attention. Last month saw claims that Tania Head, whose story of rescue from 9/11 inspired people across the world, had not in fact been employed by Merrill Lynch at the World Trade Center, did not have two degrees from Harvard and Stanford and was unknown to the family of a supposed fiancée who died when the towers came down.

If true, that imposture is an echo of people who claimed to be survivors of the Holocaust¹⁹, the *Titanic* sinking and even the Donner ‘cannibal party’ in the US²⁰.

Life after death?

Others arrange their own disappearance, at the someone else’s expense. One of the more egregious examples is that of UK member of parliament and Privy Councillor John Stonehouse.

In 1974 Stonehouse escaped from financial difficulties and marriage by faking his own death. He had taken out life insurance with five insurers, naming his wife (who was unaware of the plan) as beneficiary. He flew to Florida, folded his clothes neatly on the beach and supposedly swam to oblivion, with the expectation that his grieving widow would collect £125,000. The fraud fell apart when Stonehouse was discovered in Melbourne, along with his mistress, and was returned to the UK.²¹

Other voice, other fingers

Earlier this year we saw furore among music lovers after it was revealed that over 100 recordings by the late Joyce Hatto – an “undiscovered genius” and “greatest British pianist of the century” – were simply relabelled performances by Hatto’s competitors. That is an echo of boy band Milli Vanilli, the Bay City Rollers of the 1990s, who were revealed to be lipsynching to tracks recorded by contractors. The revelation resulted in class action and substantial payouts to deceived fans. Both incidents pose questions about what we mean by identity, authenticity and why we value it.

Those questions are evident in considering the visual arts, where there has been a long history of appropriation (for example adding someone else’s signature to ‘improve’ an existing work or creating an entirely new work purportedly by Drysdale,

¹⁸ Last month Tiffany Weaver pleaded guilty to using fake photo ID, having posed as a lawyer and entered a Baltimore prison to have sex with an inmate serving 30 years for manslaughter. Weaver successfully entered the facility using a Bar association security pass and the business card that featured the name of a real lawyer. She was charged with identity theft and use of false government identification.

¹⁹ One example is Benjamin Wilkomirski/Bruno Doessekker, author of a supposedly authentic memoir that was critically acclaimed and appeared on bestseller lists, discussed in *A Life in Pieces: the Making and Unmaking of Benjamin Wilkomirski* (New York: Norton 2002) by Blake Eskin.

²⁰ One beggar pointed to his missing leg, claiming implausibly that it had been eaten by his peers.

²¹ Stonehouse had used a false passport in the name of Joseph Markham, a dead constituent. In Melbourne he masqueraded as Clive Mildoon, another dead constituent, presumably funded by some of the £600,000 missing from his fund for Bangladesh hurricane victims.

Streeton, Bacon, Rodin or another master) and complicity by dealers in misattribution of works.²²

Payment Systems

Identity crime in payment systems dates from before the South Sea Bubble, the prototype of the dot com crash. Criminals forged bills of exchange, deeds and wills – modern forgery law derives from court judgements and statutes that aimed to preserve the integrity of the financial system and deter misbehaviour. By the 1760s for example, after a bout of anxiety that is similar to contemporary fears about electronic commerce, there were over 100 forgery offences punishable with the death penalty.²³

We are more relaxed about payment offences these days and much of the anxiety regarding payment-related identity crime appears to be misplaced. There is major disagreement about the shape and interpretation of figures for cheque and card fraud.²⁴ However, it appears that much crime is distinctly low tech, attributable to thefts of unattended wallets and bags, stealing credit card and bank statements from letterboxes or rubbish bins, ‘borrowing’ use of a card from a family member, skimming cards handed to a waiter in a restaurant and, in the UK, stealing new/replacement cards from the post.²⁵

Serial bride and supposed millionaire Emma Golightly extracted £250,000 from her lovers by borrowing their cards, alas omitting to pay for her latest wedding. UK postman Dido Mayue-Belezika led a gang that stole around £20 million, for example by intercepting chequebooks. Competitor Ali Dahir snaffled over 3,000 stolen cards, extracted from letterboxes and postal sorting rooms, to buy luxury goods worth £870,000.

Photoshop kids

This paper began by asking whether identity crime involved the kid next door? There are few comprehensive and authoritative studies of the extent to which kids are misusing proof of identity documents to get entry to clubs or other age-restricted venues. There is similar disagreement about the number of bogus passports, birth

²² cf www.caslon.com.au/forgeryprofile5.htm for comments on authenticity, economics, belief and gatekeeping.

²³ See for example the discussion in Randall McGowen’s ‘Making the ‘bloody code’? Forgery legislation in eighteenth-century England’ in *Law, Crime & English Society, 1660–1830* (Cambridge: Cambridge Uni Press 2002) edited by Norma Landau and Valentin Groebner’s *Who Are You? Identification, Deception and Surveillance in Early Modern Europe* (New York: Zone 2007). McGowen suggests that a third of all capital statutes passed in the UK between 1700 and 1830 dealt with forgery.

²⁴ Ian Woods’ 1998 Australian Institute of Criminology paper *Fraud & the Australian Banking Industry* notes uncertainties about Australian cheque fraud costs, consistent with Russell Smith’s 2003 *Examining Legislative & Regulatory Controls on Identity Fraud in Australia* and *Addressing Identity-related Fraud in the Retail Financial Services Sector papers* and the 2001 Commonwealth Attorney General’s Department *Scoping Identity Fraud* study. The American Bankers Association reported in 2000 that there were US\$679 million actual losses regarding cheque fraud and US\$1.5 billion potential losses in the preceding year. Edward Potter’s 2002 ‘Customer Authentication: The Evolution of Signature Verification in Financial Institutions’ in 1 *Journal of Economic Crime Management* 1 offers a succinct overview of authentication challenges in the US.

²⁵ In 2006 fraud in Australia on credit cards was reported as the equivalent of 37 cents per \$1,000 transacted (with fraud on PIN-based debit cards at 8 cents per \$1,000), less than a third of the rates in the UK. Payments System Board (Reserve Bank of Australia) *Annual Report* 2007, 13-14.

certificates and drivers licences in circulation.²⁶ Much media coverage is anecdotal and it is often difficult to reconcile figures from government and industry.

It is clear that some people are manufacturing birth certificates and licences, entirely sidestepping the relevant agencies.²⁷ Others are improperly gaining legitimate certificates, for example by 'rebirthing' children whose death has appeared in obituaries. Some people improperly gain legitimate documentation from associates in government agencies. Others buy or steal blank documents.²⁸

As is often remarked, that documentation can then be used to 'breed' other documents. It can also be used to deflect enforcement action by police or other regulatory bodies, with victims lamenting on occasion that their credit profile may be unsullied but they have been exhausted by the task of persuading law enforcers of their innocence and ensuring that corrections are made in the relevant databases.²⁹

'Novelty documents'

A credentialist culture – you are who your blurry photo-ID says you are – means that there is a market for fake identity cards and a minor industry to serve that market. If you have a couple of hours to kill, go online and search for 'novelty documents' ... everything from fake bank statements and utility bills or payslips to drivers licences, proof-of-age cards and even passports. Some of the document factories will whip up a bank statement for you overnight (expect to pay around £80)³⁰; some will even sell you a "fully editable template" for around £500, in the same way that you can buy templates to award yourself a degree in criminology from a real or fictitious university.

²⁶ The NSW Registry of Births Deaths & Marriages and Westpac famously reported that 13% of a sample of birth certificates were 'defective'; the interpretation of that figure is contentious. One of the major points of entry to the literature remains Russell Smith's 1998 Australian Institute of Criminology paper *Measuring the Extent of Fraud in Australia*.

²⁷ Today's *Sydney Morning Herald* for example reports that "An alleged serial fraudster bit another man in the face when he tried to repossess a vehicle containing a range of fake driver's licences, police say. The victim of the attack was repossessing the vehicle in Victoria Street, Kogarah, about 8am yesterday when its owner allegedly bit him on the face. ... A search of his vehicle allegedly turned up numerous documents in different names. ... Police said the vehicle contained three false NSW driver's licences and two New Zealand driver's licences in different names, along with several credit and debit cards."

²⁸ In 2003 for example the government of Papua New Guinea announced theft of that nation's passport database, along with computer backups and blank passports. A year later the French government revealed the disappearance of some 10,000 blank French passports, 5,000 blank French driver's licenses, 10,000 blank car ownership certificates and 1,000 international driver's licences.

²⁹ A local example is the NSW Privacy Commissioner's 1 January 2003 note 'Amending erroneous police records due to identity theft' (2003 *NSWPrivCmr* 1) regarding the experience of Mr A, who "received communications from ... government agencies which incorrectly stated that he had been charged with a number of offences and had recently been in prison. Mr A complained to the NSW Police Service. He was informed that because Mr B had given a false name when he was first charged, the Police Service criminal record system would always default to the name given on the first charge. In this case Mr A's name would head the criminal record for Mr B, even though the Police subsequently discovered Mr B's real name."

³⁰ The author has suggested that one way to crimp the document factories is for banks and other financial institutions to take action for trademark infringement, as those institutions are victims of fraud facilitated by fake documents and those documents clearly feature trademarked corporate names and logos. So far there appears to have been no litigation in Australia, New Zealand and the UK against 'novelty' sites or against the notorious www.fakealibi.co.uk, marketed as "the World's Only Legitimate Alibi Service".

Theidshop.com for example boasts

We can replicate most any passport upon request and proper pricing. Our Fake Passports are of the highest quality and look very near identical to an official one. In addition we can work on a one-on-one basic with you to create a completely custom passport job. Use our fake passports in conjunction with our fake ID's for a complete "New Identity" Package. Upon request we can create a complete identity solution. This can include a fake novelty id, fake passport and several other different forms of identification such as credit cards, checkbooks, utility bills and fake corporate documents if needed. Let us stress that creating our custom packages are only for individuals that are serious about creating complete turn key identify packages.

Vendors of such documents hide behind formal cautions that their 'facsimile' is a novelty, not the real McCoy, and that "without exception are not to be used for financial gain, deception, fraud or other criminal activity". £500 is a lot of money for a novelty.

Criminals with a bit more savvy or cash will, of course, continue to buy passports and other documents from corrupt officials (money laundering and terrorism experts have expressed concern about practice in some of our neighbouring countries) or as noted above buy blank documents stolen/lost from government offices.³¹

Joe jobs and sock puppets

Forging an email address is a trivial task. One of the nastier identity crimes plays on consumer unfamiliarity with technology (and the desire to believe) by sending email that purports to come from a politician, an academic, a human rights advocate or other figure but instead originates with an ill-wisher or a commercial scammer. The offender has appropriated the victim's identity in engaging in 'joe jobs' – email that aims to erode the supposed sender's reputation (bringing the person into disrepute, feeding media speculation and causing recipients to block legitimate messages).

Joe jobs in the past five years have included fake outing of UK and US politicians, defamatory communications attributed to socialites and false statements attributed to Noam Chomsky, Hilary Clinton and others.³² They are a form of identity crime that is likely to become more prominent in coming years.³³

³¹ Networked verification mechanisms mean that some of those documents will not get the bearer across the border. However, they may be instrumental in allowing the bearer to open bank accounts, apply for other documents and so forth. Unfortunately there is no authoritative public data on misuse and a recurrent complaint in overseas official reports is that different agencies do not talk to each other – or merely wash their failures in public – regarding who is using illicit passports and how they are using them.

³² For a discussion of online defamation, pseudonymity and identity appropriation see www.caslon.com.au/defamationprofile.htm. For examples of joe jobs see Abby Aguirre's 28 October 2002 'Palestine Activism Spammed' in *The Nation* at www.thenation.com/doc/20021028/aguirre.

³³ Email joe jobs are a descendent of traditional mail-outs. The past two years in the US have seen automated telephone calling with recorded messages that purport to come from or in support of political figures and rights advocates, fuelling suggestions that the US Do Not Call regime should be extended to restrict all political 'robocalls'. Observers of cyberbullying have expressed concern about kids sharing passwords as 'best friends' and then engaging in editing of personal profiles in online social spaces such as MySpace or sending nastygrams that purport to come from a now former best friend (aka fbf). In the digital environment some identity crime involves a gasp of horror from a nine year old rather than misuse of a credit card.

Joe jobs may also be used to boost/depress share prices and derail takeovers. Many online fora do not impose onerous identification requirements for entry or ongoing participation, often only needing an email address (one that might be from a 'use once and throwaway' webmail service such as Hotmail that itself requires no validation). Much participation is pseudonymous: Participants can also communicate in the guise of another individual or as representative of an organization, a comment that will not surprise anyone who has received '419' spam claiming to come from the heirs of Arafat and sundry African tyrants³⁴ or offers of discount software and medications that purportedly come from the World Bank, Sorbonne, Australian Federal Police, Reuters or the Red Cross. Some communicate as 'sock puppets', with an individual adopting different personas in the same forum to endorse comments or requests made using one of the identities.

On the net, to adapt the famous *New Yorker* cartoon, many people can't tell that you are a dog and appropriation is often just a click away because people lack the tools required for sniffing each others tails. A 2003 *Boston Globe* article ironically suggested

Looking for revenge on that rotten former boyfriend? Make a homepage in his name where he brags about being a liar and ex-con with scabies. Let Google do the rest ...

That suggestion has been taken at face value by disgruntled ex-lovers in the US, UK, Japan and elsewhere.

Pretexting

The preceding paragraphs have highlighted examples of offences against insurers and other organisations. It is clear, however, that insurers, leading law firms and pillars of the corporate community in the UK, Canada and US have exploited information gained through identity crime – what has variously been characterised as pretexting or blagging.³⁵ Recent complaints by private investigators suggest that such activity is occurring in Australia.³⁶ It is a deeply traditional practice that in essence involves seeking personal information, such as phone and travel records, in the guise of the person to whom that information relates.

Organisations have typically indicated that any offences are not their responsibility: they are merely buying information from a contractor and like Inspector Renault in *Casablanca* are shocked, shocked to discover misbehaviour. That has attracted criticism in the US.³⁷ The UK appears to be moving towards commercially meaningful

³⁴ An itemisation appears at www.caslon.com.au/419scamnote2.htm

³⁵ Incidents have involved Mishcon de Reya (the high profile UK lawyers known for handling Princess Diana's divorce and defending Deborah Lipstadt in defamation action by Hitler enthusiast David Irving), US information technology giant Hewlett-Packard, leading insurer CNA, General Motors UK and Dakin.

³⁶ John Bracey, president of the Australian Institute of Private Detectives, was reported as commenting in October 2006 that "asking a private detective not to use such surveillance methods is like asking a carpenter to put cupboards up without using a hammer, nails, screws or a saw." cf *The Law of Private Security in Australia* (Pymont: Law Book Co 2005) by Rick Sarre & Tim Prenzler. Frederick Cantz Jr's 2007 'Lessons From Hewlett-Packard: The Legal and Ethical Implications of Investigating Suspected Fraud' in *Pennsylvania Lawyer* (March/April) 43 notes that "Some of the investigative tactics in the HP case are considered acceptable methods of obtaining information, even though they may not look particularly good under scrutiny", with dumpster diving for example being "Unseemly but OK".

³⁷ The US Federal Trade Commission notes at www.ftc.gov/bcp/online/pubs/credit/pretext.htm that "Pretexters use a variety of tactics to get your personal information. For example, a pretexter may call,

restrictions on sale and use of such data, after strong criticism by the Information Commissioner (counterpart of Australia's Federal Privacy Commissioner), a move that is likely to have some influence in Australia.

Custodians

One source of information for identity criminals is, alas, the organizations that have been entrusted by consumers with their personal information.

A recent article for *Privacy Law Bulletin* noted³⁸ that literally hundreds of millions of consumer files (including credit card and bank account details, social security numbers, contact details and medical records) have been exposed by organizations that include –

- service providers such as iBill (the online adult content billing service, with some 18 million cards), CardSystems Solutions (over 40 million credit cards), WellPoint (196,000 records) and ChoicePoint
- leading financial and insurance institutions such as BankofAmerica (1.2 million cards), JP Morgan Chase (2.6 million accounts), Canadian Imperial Bank of Commerce (470,000 mutual fund customers), Ameritrade (200,000), American International Group (930,000 customers), ING and Citigroup (3.9 million active/closed accounts)
- major accounting businesses and organizations such as E&Y (243,000 customers), Deloitte & Touche and the American Institute of Certified Public Accountants (230,000 members)
- the US federal government and state governments, eg Georgia Department of Health (records on 2.6 million people) and US Veterans Administration (26.5 million people)
- major universities such as the University of California San Diego (1.4 million records), UCLA (800,000 personal records) and Ohio University (173,000)
- leading enterprises such as Time Warner (600,000 records), Polo Ralph Lauren (180,000 records), Marriott Vacation Club (206,000 employee and customer records) and retail conglomerate TJX (45.6 million accounts).

claim he's from a survey firm, and ask you a few questions. When the pretexter has the information he wants, he uses it to call your financial institution. He pretends to be you or someone with authorized access to your account. He might claim that he's forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain personal information about you such as your SSN, bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios." Supporters of the pre-2007 US regime noted that breaking into online accounts violates the *Computer Fraud & Abuse Act* (18 USC 1030) and that pretexting that deceives network operators to provide 'private' information violates the *Wire Fraud Act* (18 USC 1343), although a caution is supplied in Jennifer Granick's 2006 'Faking It: Calculating Loss in Computer Crime Sentencing'. The federal *Telephone Records & Privacy Protection Act of 2006* (TRPPA) provides up to 10 years imprisonment for anyone who pretends to be someone else, or otherwise employs fraudulent tactics, to persuade telcos to hand over what is supposed to be confidential data about customers' calling habits. It is underpinned by FCC rules of April 2007 that require network operators to adopt safeguards to protect personal telephone records from unauthorised disclosure. Carriers are required to notify customers immediately when changes are made to their account and notify customers in the event of a breach of confidentiality. An industry spokesperson, critical of restrictions on providing marketers with customer information, sniffed that "this is an extremely anticonsumer outcome".

³⁸ Bruce Arnold 'Losing IT – Corporate Reporting on Data Theft', *Privacy Law Bulletin* (March 2007). There is a more detailed discussion at www.caslon.com.au/datalossnote.htm

Some of that exposure results from hacking or sale of information by insiders. Other exposure seems strikingly negligent, with unencrypted disks and tapes being lost in transit (some appear to have literally fallen off the back of the truck), laptops³⁹ and hard drives recurrently going AWOL from homes and offices, and data being sold to front companies.

Some of the missing tapes have probably ended up as landfill and some devices have presumably been scrubbed: the thief wanted the box, not the data contained therein. However, it is clear that some personal information is being actively used by criminals – with consumers and industry bearing the cost through chargebacks and the pain of resolving disputes – and that much of the loss is preventable.

Are businesses in Australia being similarly derelict? The short answer is that we do not know. There are no public reporting requirements, in contrast to the US where disclosure of data losses is attributable to mandatory reporting under state and federal law. That reporting is becoming increasingly sophisticated, and of course underpins commercial services marketed to consumers who are at risk of identity crime.⁴⁰

■ costs

What are the costs for business of identity crime?

Media coverage typically focuses on direct financial losses: money that goes missing when an insider perpetrates an offence, losses that are made when a customer scams an organization.

It is important, however, to look at total costs. For a corporation or government agency they include –

- erosion of reputation, including loss of business from consumers, avoidance by potential partners, reduced credibility in dealing with government and higher insurance premiums
- remedial action, in particular the cost of retrofitting security systems
- penalties imposed by government regulators or industry regulators
- damages imposed by courts, whether on an individual or class action basis
- the cost in management time and legal services of defending litigation.⁴¹

³⁹ In Australia the Minister for Defence acknowledged in 2000 that around 1.8% of the 7,000 laptops used across his portfolio went AWOL each year, claiming that "the portable computer loss rate in the private sector is much higher at between 10% and 15%". That acknowledgement is useful as an indication that loss is not restricted to the private sector. Answers to Parliamentary Questions subsequently revealed that during 2003 some 90 desktop and 25 laptop computers were either stolen or lost from Australian defence establishments, up from 73 laptops and 105 desktop machines in 2001 (of which 13 held classified information and three held commercially sensitive information). In 2000 the Defence Department reported that 54 laptops were lost and 73 stolen. During the following year some 650 federal government computers were reported stolen, with 30 laptops missing from ASIO, the National Crime Authority and the Australian Federal Police. At that time the FBI was losing around 11 laptops per month.

⁴⁰ The Australian Democrats recently proposed national legislation regarding mandatory reporting; that suggestion has gained little attention but it is likely that the US model will be adopted in the next five years on an opportunistic basis.

⁴¹ In the US, for example, there has been class action against Toys 'R' Us, Quick-Chek (convenience stores), Hess (petrol), Avis and Budget (car rental), IKEA (furniture), Costco, Victoria's Secret (lingerie) and Rite-Aid (pharmacies) over credit-card and debit-card sales receipts that "disclose too

We can get some sense of those costs by noting overseas responses to overseas incidents.

The UK financial services regulator for example imposed a £980,000 penalty on Nationwide, that country's largest building society, over loss of a laptop that held unencrypted data on 11 million customers.⁴² Choicepoint, noted above, received a US\$15 million penalty from the US regulator after selling some 145,000 records and is currently facing class action amid announcements that key clients are reconsidering their relationship.⁴³ The chief executive of credit card processor CardSystem Solutions complained that the business was facing "imminent extinction" after it was revealed that hackers had accessed 40 million card details.

The US Veterans Administration announced that it had budgeted US\$25 million for a special call centre and mailouts after it lost a laptop containing unencrypted information about 26.5 million people.

Retailer TJX announced yesterday that its first-quarter profit dipped 1% as initial costs related to "a widely publicized breach of customer data" offset revenue growth.⁴⁴

■ impacts and uncertainties

How much does identity crime cost the Australian economy and community?

One answer is that we simply do not know.⁴⁵

much information". The litigation reflects the *Fair & Accurate Credit Transactions Act* (FACTA) (15 U.S.C. 1681c(g)(1)) that prohibits listing on an electronically-generated receipt of the expiration date or more than five digits of the account number from the consumer's credit or debit card, with the merchant exposed to damages of up to US\$1,000 per infraction. The American Federation of Government Employees recently filed a class action lawsuit against the Transportation Security Administration (TSA), the federal agency responsible for safeguarding US airports, after loss of an external hard drive containing personal and financial information of 100,000 current and former employees. The union contends that loss is a breach of the *Privacy Act* of 1974 and the *Aviation & Transportation Security Act*.

⁴² UK regulator the Financial Services Authority, in imposing a £980,000 penalty, criticized the organization for a delay of three weeks in investigating the significance of the loss. It commented that "Nationwide is the UK's largest building society and holds confidential information for over 11 million customers. Nationwide's customers were entitled to rely upon it to take reasonable steps to make sure their personal information was secure."

⁴³ For a perspective see Flora Garcia's 2007 'Data Protection, Breach Notification and the Interplay between State and Federal Law: The Experiments Need More Time' in 17 *Fordham Intellectual Property, Media & Entertainment Law Journal* (Spring 2007), 693-726.

⁴⁴ The 15 May 2007 Toronto *Globe & Mail* reported that TJX "said it will incur more costs related to the investigation, enhancing computer security and systems, as well as technical, legal and other fees that could total 2 or 3 cents per share in the second quarter. Beyond these costs, TJX said it doesn't know how much the data breach will eventually cost, including exposure to credit card companies and banks, various legal proceedings and other expenses."

⁴⁵ The Australian Federal Attorney General's Department 2001 *Scoping Identity Fraud* study commented that "There is widespread agreement by all organisations that identity fraud already represents a significant problem, that is likely to grow further. The lack of statistics on the incidence and cost of identity-related fraud makes the total cost to the community impossible to accurately quantify. Without reliable estimates of the overall cost it becomes more difficult to convince decision-makers that urgent attention is required". That is consistent with Russell Smith's 1998 Australian Institute of Criminology *Measuring the Extent of Fraud in Australia* paper.

That is partly because of disagreement about definitions. It is partly because many incidents do not appear in the public domain.

The US Federal Trade Commission estimates that identity-related offences cost US consumers and businesses US\$53 billion in 2002, with Governor Arnold Schwarzenegger indicating in 2005 that financial costs for that year were around US\$57 billion.⁴⁶ *Industry Fraud in Australia*, a 2003 report by the Securities Industry Research Centre of Asia-Pacific (SIRCA) claimed that identity fraud cost the Australian community \$1.1 billion in 2001/2, with roughly 50% concerned with 'response activity'.⁴⁷

The UK Cabinet Office, noting difficulty in estimating identity crime costs, commented that the minimum was £1.3 billion. In 2006 the Home Office estimated that the annual cost of identity crime was £1.7 billion, a figure dismissed by the Association of Payment Clearing Services (APAC) as too high, claiming that card fraud was worth £37 million in 2004 rather than £504 million.

In 2005 the Australian federal Attorney-General reported one estimate that identity fraud cost the local banking industry a mere \$25 million per year. That is consistent with figures in the 2002 KPMG *Fraud Survey* and the 2003 Australian Institute of Criminology & PWC *Serious Fraud in Australia & New Zealand* study. In the latter study, based on a sample of 155 cases, false documents were used in 69% of cases (15% involving cheques) and identity fraud was evident in 36% of cases (13% with "stolen identities" and 25% with wholly false identities).

The Australian House of Representatives Standing Committee on Economics, Finance & Public Administration (EFPA) *Numbers on the Run* report expressed concern at the lack of definitive figures regarding the extent and cost of identity crime but noted that 25% of frauds reported to the Australian Federal Police involved false identities. That figure was characterised as biased towards the sort of crime reported to the AFP, in particular welfare fraud.

US scholar Chris Hoofnagle commented two months ago that

There is widespread agreement that identity theft causes financial damage to consumers, lending institutions, retail establishments and the economy as a whole. Surprisingly, there is little good public information available about the scope of the crime and the actual damage it inflicts. The publicly available data on identity theft come mainly from survey research. Methodologically, these survey polls of the public suffer from being both under- and over-inclusive in measuring the problem. As a result, low estimates attribute tens of billions of dollars to the economy and consumers, the highest estimates place losses in the hundreds of billions.

To identify proper interventions and appropriately allocate resources we need comprehensive, hard data on the scope and effect of identity theft.⁴⁸

⁴⁶ California has led US government responses to identity crime over the past decade, with the states often being more activist – and arguably more effective – than agencies in Washington.

⁴⁷ Suresh Cuganesan & David Lacey's 2003 'Identity Fraud in Australia: An evaluation of its Nature, Cost and Extent' for SIRCA suggested \$1.1 billion as the cost to the Australian community of "identity fraud".

⁴⁸ Chris Hoofnagle, 'Identity Theft: Making the Known Unknowns Known' in 21 *Harvard Journal of Law & Technology* (2007).

Another answer is that much crime reporting and much policing is biased towards offences that can be quantified, particularly quantified with a financial value. We do not quantify the pain suffered by a parent whose dead child has been rebirthed by an identity thief; that pain is not recognised in Australian law. We also do not quantify the humiliation or anxiety suffered by someone who discovers that their name has been 'borrowed' or their photo has been scraped from a site such as Flickr.com or Facebook, although the victim may have a remedy under intellectual property or passing off law.⁴⁹

■ law

Belief that identity crime is an unprecedented phenomenon has been reflected in perceptions that there is a need for an identity crime enactment or that such a law already exists.

In fact there is no discrete identity theft/fraud law that covers all offences, whether at the national or state/territory level. Instead, as you might expect from the preceding paragraphs, identity crime in Australia is addressed through a wide range of statutes and common law. Much of that law is quite old and quite specific.⁵⁰

There is a broad demarcation between federal law and state/territory law, with inconsistencies in the characterisation of offences and questions about penalties and jurisdiction in enforcement. Some offences are dealt with under discrete enactments such as the federal financial transactions reporting legislation.

Most are addressed under the federal and state/territory Criminal Codes or Crimes Acts, which feature offences characterised as –

- Fraud
- Supplying false information
- Attempting dishonestly to gain a financial advantage
- False Pretences
- Obtaining credit by fraud
- Falsification of documents
- Making a false instrument
- Unlawfully altering data processing material
- Forging
- Using forged documents
- Uttering
- Preparation for Forgery
- Obtaining money by false or misleading statements

⁴⁹ For scraping see the discussion at www.caslon.com.au/photonote15.htm.

⁵⁰ Two of the more lucid discussions of the overall regime are provided by Simon Bronitt & Bernadette McSherry in *Principles of Criminal Law* 2 ed (Pymont: Lawbook Co 2005) and by David Lanham, Bronwyn Bartal, Robert Evans & David Wood in *Criminal Laws in Australia* (Leichhardt: Federation Press 2006). A point of entry to US literature regarding redress and corporate liability is provided by Anthony White's 2005 'The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going To Pay For It?' in 88 *Marquette Law Review*, 847-866. There is a useful overview of the Australian regimes at 393-401 of the Australian Law Reform Commission 2007 *Review of Australian Privacy Law Discussion Paper* (v 1).

- Impersonation of a Commonwealth Officer
- Producing False Records.⁵¹

Those provisions encompass offences regarding land titles⁵², pharmaceutical benefits⁵³, cheques⁵⁴, education⁵⁵, taxation, income support and so forth. They are complemented by a wide range of other statutes.⁵⁶ Statutory and common law obligations continue to evolve.⁵⁷

It is also useful to recognise the value of contract law, with organizations for example dismissing employees who have knowingly supplied false information (or omitted particular information) during recruitment or promotion.

How is the legal landscape changing?

Australia is likely to move, albeit slowly, to mandatory disclosure of corporate data losses. That may be welcomed by some parts of the insurance industry (and of course by security service providers) as encouraging business best practice. Adoption by over 30 US states of credit reference 'freeze law' is likely to be more controversial. That legislation freezes access to consumer credit reports when requested by a consumer who has been affected by identity theft.

Freezing is a measure of desperation: banks and other lenders will not provide credit when they do not have access to the report. Consumers have agitated for freezing after a large number of high profile incidents where an identity criminal has appropriated an individual's identity, mortgaged a property or simply racked up loans and credit card debts and then disappeared, leaving the victim to bear the pain.

■ other responses

⁵¹ South Australia's *Criminal Law Consolidation (Identity Theft) Amendment Act 2004* is the only specific 'identity crime' enactment. It provides that assuming a false identity of another person - living or dead, real or fictional, natural or corporate - makes a 'false pretence', even if the person acts with the consent of the person whose identity is falsely assumed. Making a false pretence with the intention of committing or facilitating commission of a serious criminal offence is in itself an offence, whether or not that crime occurs. The 2004 Act also encompasses production or possession of material (including personal identification information) that enables a person to assume a false identity.

⁵² cf Sharon Roderick's 2002 'Forgeries, False Attestations and Impostors: Torrens System Mortgages and the Fraud Exception to Indefeasibility' in 7 *Deakin Law Review* 1, 97-130 and Peter Butt's 2001 'Mortgages and the paperless register' in 75 *Australian Law Journal* 7, 406-407.

⁵³ cf Peter Dwyer's 2001 'Pharmacist as prescriptions custodian' in 9 *Australian Health Law Bulletin* 6, 58-59

⁵⁴ cf Marion Hetherington's 1996 'Responsibility for payment of forged cheques: lessons from NAB v Hokit' in 7 *Journal of Banking & Finance Law & Practice* 4, 313-314; Sharon Christensen, William Duncan & Rouhshi Low's 2003 'The Statute of Frauds in the Digital Age - Maintaining the Integrity of Signatures' in 10 *Murdoch University Electronic Journal of Law* 4 and Tim Carmody's 1998 'False documents and fictional characters in Queensland' in 22 *Criminal Law Journal* 4, 215-226.

⁵⁵ cf Russell Smith's 2006 'Criminal misuse of identity in higher education' in 2 *Privacy Law Bulletin* 9, 124-12

⁵⁶ Examples in relation to impersonation include s75 *Tow Truck Industry 1998* (NSW), s66 *Jury Act 1995* (Qld), s126 *Gas Act 2000* (Tas), s18 *Fertilizers Act 1993* (Tas), s140 *Electricity Safety Act 1998* (Vic), s175 *Chiropractors Registration Act 2001* (Qld), s24 *Court Security Act 2005* (NSW), s32 *Status of Children Act 1996* (NSW) and s95 *Pest Management Act 2001* (Qld).

⁵⁷ As noted in Lloyd Nash & Sarah Gaggin's 'Queensland mortgagees beware' in 20 *Australian Property Law Bulletin* 7, 81-83, the *Natural Resources & Other Legislation Amendment Act 2005* (QLD) for example imposes substantial new obligations on mortgagees in Queensland to take 'reasonable steps' to verify the identity of the mortgagor signing the mortgage document.

Law is not a silver bullet that eliminates self-help by consumers, best practice by organizations and use of technological enablers. It has some deterrent value in encouraging best practice among data custodians but overall provides a remedy once identity crime has occurred, not before.

Consumer technologies

Technology vendors have argued that much identity crime, in particular online crime, can be effectively addressed through solutions such as fobs and biometric-equipped keyboards or ancillary devices.

Consumers have been reluctant to embrace that vision and appear unlikely to do so in future unless the technology becomes more user friendly, is more accurate (real world performance is typically much lower than reported results from laboratories) or is forced on the consumer by retailers and financial institutions.

Forcing appears unlikely, given tacit recognition within many institutions and parts of government that the internet begins at the consumer's fingertips, rather than behind a remote firewall that is rigorously guarded by experts. (Sceptics of course note some of the incidents highlighted above in questioning the efficacy of some guards). It is clear that some consumers will continue to blithely disclose information through phishing, discussed in more detail elsewhere as part of the MOSC program.

Most will continue to use devices that critics such as e-commerce security expert Bill Caelli characterise as unfit for purpose ... and unlikely to get fitter while we have a monoculture centred on using consumers as bug-testers and shifting costs to those consumers.⁵⁸

Consumer education

In practice consumer education, and more broadly consumer self-help, offers a useful response to a range of identity crime.⁵⁹

Much self-help is distinctly low-tech but appears likely to be effective in reducing both the incidence and severity of identity crime. It includes such things as –

- reading your financial statements on an ongoing basis, rather than just at the end of the financial year or near the BAS deadline
- shredding used financial documentation or storing it securely
- encouraging data custodians, including employers, to adopt best practice in data handling (one way to crimp the dumpster diving evident in the Sydney, Melbourne and Canberra CBD)
- safeguarding bags, wallets, memory sticks and laptops.

Takedowns

⁵⁸ For the economics of e-commerce security see 'The Law and Economics of Software Security' by Robert Hahn & Anne Layne-Farrar in the *Harvard Journal of Law & Public Policy* (2006), Ross Anderson's 2001 *Why Information Security is Hard: An Economic Perspective* and Lawrence Gordon & Martin Loeb's 'The Economics of Information Security Investment' in *Economics of Information Security* (Dordrecht: Kluwer Academic 2004) edited by L Jean Camp & Stephen Lewis.

⁵⁹ George Milne's 2003 'How Well Do Consumers Protect Themselves From Identity Theft?' in 37 *The Journal of Consumer Affairs* 2, 388-402

AusCERT, in submissions to auDA (the independent body responsible for the Australian domain name system)⁶⁰, has asked whether it is appropriate and feasible to inhibit some internet-based identity crimes – such as phishing – through special powers that would allow a national regulatory body to quickly ‘take down’ sites that were reasonably believed to be used for improper purposes.⁶¹ An ‘instant response’ is attractive to some policymakers, who have lamented delays in responding to some online offences but poses substantial challenges under existing Australian law. It would of course not be effective against sites that are outside Australia’s jurisdiction.

■ recent developments

Identity crime is not going to disappear. It is therefore worth considering how the regulatory environment may evolve.

Law Reform

Earlier this year we saw release of an *Identity Crime* issues paper by the Model Criminal Law Officers’ Committee (MCLOC) of the Standing Committee of Attorneys-General (aka SCAG).

Some readers of this paper will be familiar with the MCLOC as the Model Criminal Code Officers Committee (MCCOC), a body of national and state/territory officials concerned with development of the model criminal code. The expectation is that the variation in common and statute law highlighted above can be addressed through adoption of a standard codification of common law and statute law regarding criminal offences.

In December 1995 the Committee released a Final Report on *Theft, Fraud, Bribery and Related Offences*. That document provided recommendations for model fraud offences including obtaining property by deception; obtaining a financial advantage by deception; production, use and possession of a false document and possession of a device for making false documents. In February 2006 it released a Final report on *Credit Card Skimming* and related offences.

The new discussion paper, likely to result in a Final Report in 2010, seeks comment on suggestions for a uniform approach to identity crime offences in all Australian jurisdictions.

Consideration of those recommendations is likely to intersect with the federal government’s response to the major report on *Privacy* by the Australian Law Reform Commission, due in 2008.

Australia Card II

The national government services Access Card, accurately described as the Australia Card II, will have some impact in reducing identity crime regarding Commonwealth and state/territory government services, although its cost

⁶⁰ The author is a member of the auDA policy body examining changes to domain name rules and structures in dot-au. auDA has strongly encouraged input from law enforcement agencies.

⁶¹ Background is at www.auda.org.au/pdf/sub-auscert.pdf and www.auda.org.au/2007npp/2007npp-index/

effectiveness remains problematical and (like overseas counterparts) appears to be deteriorating.⁶²

Private sector use – or misuse – of the Access Card is currently something of a ‘monster under the bed’: we think it is there, it is scary, we do not want to provoke it by looking too closely.

In practice it is almost certain that the Card will become the *de facto* identity document for a wide range of private sector transactions, replacing the driver’s licence as the photo ID that you hand over when renting a video, buying an airline ticket, getting into age-restricted premises or opening a bank account.⁶³

In the absence of online verification it is unlikely that the Card will substantially reduce identity crime in the private sector over the long term. It is a useful tool, rather than a silver bullet, and the challenge facing many proponents is to contain unrealistic expectations.⁶⁴ We can expect to see fake Cards in the same way that we have seen fake drivers licences and other proof of identity documents.

Insurance

Someone’s pain is often another’s potential gain. It is unsurprising that we are seeing the emergence of commercial services directed at consumers who may be the victims of identity crime or at organizations whose handle consumer data.⁶⁵

Some services offer insurance, either a substantial payment to cover serious losses or a smaller payment to cover the cost of contact with banks and other organizations when the consumer believes that identity crime has occurred (or is likely to occur because a data custodian has exposed the individual’s information).⁶⁶

The dominant consumer credit reference services have meanwhile actively marketed identity crime alert services, on the basis that consumers will be informed if there is unusual activity relating to their personal profile (eg that someone gains five credit cards and takes out several loans, a potential indicator that an identity is being appropriated).

⁶² See for example ‘Australia’s proposed ID Card: Still Quacking Like A Duck’ by Graham Greenleaf in *UNSW Law Research Series 1* (2007), ‘Identity Management: Is an Identity Card the Solution for Australia?’ by Margaret Jackson & Julian Ligertwood in *24 Prometheus 4* (December 2006) and www.caslon.com.au/australiacardprofile.htm.

⁶³ Restrictions on private use of the Access Card are analogous to those regarding privacy: consumers will not be obligated to provide the Card but will be able to choose to use it as a proof of identity, consistent with government promotion that “it is your card”.

⁶⁴ The recent AIC paper by Kim-Kwang Choo, Russell Smith and Rob McCusker on *Future directions in technology-enabled crime: 2007–2009* notes at page 105 that “Developments in government access cards and biometric passports ... could be exploited by organised criminal groups that seek to compromise the underlying infrastructure, or others who seek to obtain personal information for use in identity-related crimes”

⁶⁵ See for example the 2006 report by SIFT Information Security on *The Economic Viability of Cyber Insurance: Seeking Financial Certainty in IT Security*.

⁶⁶ Major US organizations have been offering customers free enrolment in a credit-monitoring service for 90 days following data losses. Critics have commented that such offers, while better than nothing (and presumably useful in heading off action by activist regulators in California and elsewhere), are inadequate as the average time for victims to become aware of database-related identity theft is 12 months, with a further 175 hours and US\$808 out-of-pocket expenses spent clearing their names.

It is important to note that some services are generating a backlash, with criticisms in the US for example by Consumers Union⁶⁷ (a counterpart of the Australian Consumers Association) and in mainstream media such as the *New York Times*.⁶⁸ Critics typically argue that –

- the alerts are ineffective, for example that consumers are not warned about ongoing suspect activity until it is too late, or even misleading⁶⁹
- credit reference services owe a duty of care to consumers rather than merely to commercial clients
- services are failing to take the basic steps that would identify instances where thieves are subverting monitoring arrangements (eg by using one person's social security number but another's name, particularly where the same number is in use with five or more names).

⁶⁷ cf www.consumersunion.org/campaigns/learn_more/003484indiv.html

⁶⁸ eg Eric Dash 'Protectors, Too, Gather Profits From ID Theft' in 16 December 2006 *New York Times*, noting suggestions that credit monitoring in the US may be a US\$900 million industry that is growing by 20 percent per year. Dash notes that "In addition to selling files to lenders in bulk, [credit] bureaus now market largely the same records to individuals, including entries that reflect applications for credit, new accounts or balance changes. While the data is sold to a big financial institution for 20 cents to \$1 a report, according to analysts and industry executives, it can be repackaged and sold to consumers in the form of credit monitoring for \$3 to \$16 a month." cf Sarah Ludington's 2006 'Reining in the Data Traders: A Tort for the Misuse of Personal Information' in 66 *Maryland Law Review*, 140-192 and discussion of the data trading industry at www.caslon.com.au/infobrokersnote.htm

⁶⁹ *ibid* notes the experience of Melody Millett, understandably surprised when her car loan provider asked if she was the wife of Abundio Perez, who had applied for 26 credit cards, financed several cars and taken out a home mortgage using a social security number belonging to her actual husband. Millett had "subscribed to a \$79.99-a-year service from Equifax, a big financial data warehouse, that promised to monitor any access to her credit records. But it never reported the credit activity that might have signaled that they were victims of identity theft". Millett is reported as saying "I feel like the whole thing is a sham", claiming that the couple received no notice of unusual access to or misuse of their credit records – "quite the contrary, the bureaus sent them a succession of reassuring e-mail messages suggesting that their information was safe and offering congratulations". Litigation is of course underway.

■ the presenter

Bruce Arnold is an information and technology law specialist with a particular interest in privacy, biometrics, online security and commercial confidentiality.

His writing appears in journals such as *Privacy Law Bulletin*, *Technology & Business* and *Security Solutions Management*.

He has been cited in over seventy books, including *Utilizing and Managing Commerce & Services Online* (2006), *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services & Identity Management* (2005), *Psychology & the Internet: Intrapersonal, Interpersonal and Transpersonal Implications* (2006), *Clinical Research Law & Compliance Handbook* (2005) and *Privacy: What Developers & IT Professionals Should Know* (2004).

He has also been cited in a wide range of government, industry and academic reports, journals and web sites, including *Proceedings of the 11th UN Congress on Crime Prevention & Criminal Justice*, Harvard Law School, *Australian Financial Review*, Australian Institute of Management's *Management Today*, Forum of Incident Response & Security Teams, CPA Australia *In the Black*, European Commission, *Wall Street Journal*, OECD Working Party on the Information Economy, *Health Information Management Journal*, Australian Institute of Criminology, Canadian Standards Association, London School of Economics, *Revue Internationale de Semiotique Juridique*, Australia New Zealand Standing Committee of Officials of Consumer Affairs, *Journal of Electronic Commerce in Organizations*, Australian Parliamentary Library, UK Information Commissioner, *Journal of Information Law & Technology*, Australian Institute of Commercialisation, *British Medical Journal* and Australian Department of Communications, Information Technology & the Arts.

Bruce has consulted to government and the private sector, including the national Department of Foreign Affairs & Trade and Department of Health & Ageing (on health data security and authentication).

He has been an invited speaker at events run by Australian and overseas governments (eg the Victorian state Justice Department) and by business on issues such as intellectual property, security, accessibility and privacy.

He has also served as an expert witness in commercial litigation and as a member of industry policymaking bodies, for example those for auDA (the Australian internet domain name regulator).

— contact details are at www.caslon.com.au —