Online IDENTITY THEFT and the law

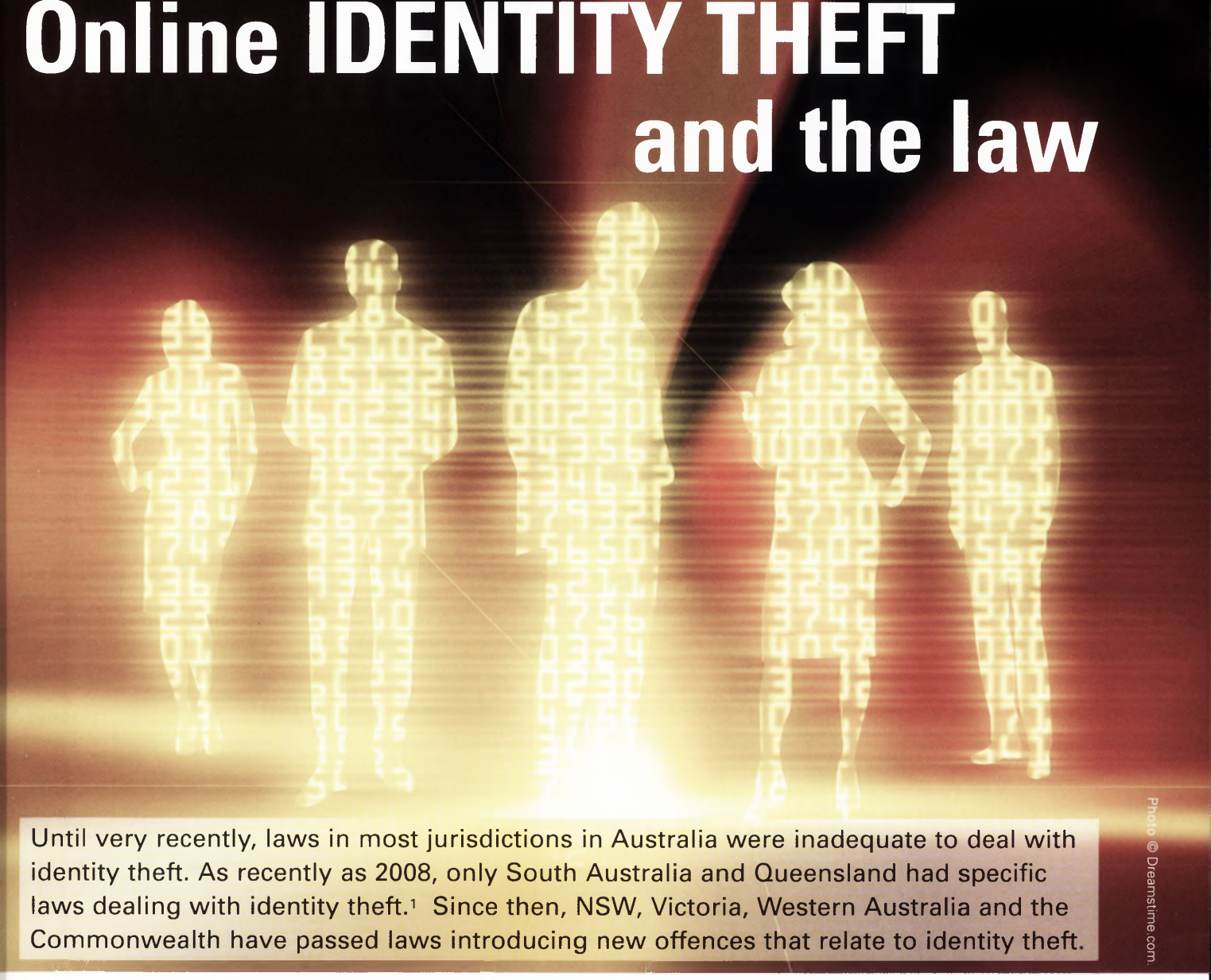

Photo © Dreamstime.com.

Until very recently, laws in most jurisdictions in Australia were inadequate to deal with identity theft. As recently as 2008, only South Australia and Queensland had specific laws dealing with identity theft.[1] Since then, NSW, Victoria, Western Australia and the Commonwealth have passed laws introducing new offences that relate to identity theft.

This article examines identity theft in the context of the internet and briefly highlights recent legislative developments in this area.

WHAT IS IDENTITY THEFT?

The Australian Law Reform Commission's Australian Privacy Law and Practice Report, tabled in August 2008, confirmed that there was 'little consensus about the definition of the term "identity theft"'.[2] Until recently, there was no specific offence that dealt with identity theft.

The Cybersmart government website defines 'identity theft' as 'when your personal information is used without your knowledge or permission'.[3] Such a definition does little to assist understanding of what amounts to identity theft, as it does not focus on the *unauthorised use* of someone's identity. This definition is also inconsistent with the National Privacy Principles, which permit disclosure of personal information in circumstances without an individual's express or implied consent.[4] By contrast, the OECD definition better captures the nature of identity theft by defining it as something that 'occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes'.[5]

ONLINE DANGERS

Identity theft has existed for a long time.[6] However, with the advent of the internet, online identity theft has represented an ever-increasing proportion of identity theft.[7] Identity fraud is believed to be Australia's fastest growing crime, with hundreds of thousands of victims and an estimated cost of more than $1 billion per year.[8]

Social networking websites, such as Facebook, LinkedIn, MySpace and Twitter have become very popular and >>

lucrative. According to a web analytics site, Facebook is the second most visited website after Google, and YouTube is third.[9] The most popular of all such social networks, Facebook, has recently been valued at about US$83 billion and has over 500 million registered users.[10]

Two of the most obvious online hazards for the public are online social networks and dating sites. From an online security viewpoint, many users fail to take adequate steps to protect their privacy online, and consequently leave themselves exposed to fraudsters who can extract and compile the kind of sensitive and valuable personal information that enables identity theft to occur. In these circumstances, the high patronage of such websites presents many opportunities for fraudsters to obtain personal identification information of individuals using those websites.

The risk of not using adequate safeguards was illustrated when an online dating site used a technique called 'website scraping' to take 250,000 user profiles from Facebook.[11] Website scraping is a software technique for extracting information from websites.[12] Although Facebook has threatened legal action against the online dating site, LovelyFaces.com, it remains unclear whether Facebook has a valid cause of action despite its terms of use prohibiting scraping.[13] So, although the conduct of LovelyFaces.com may be legal, it illustrates the opportunities available for obtaining the personal information of internet users.

In a similar way, online dating represents another potential hazard for users who place personal information about themselves online. The risks for the public are sufficient for regulatory authorities in Australia and the US to provide tips for users of such sites about how to reduce the risk of identity theft.[14]

CAN ORGANISATIONS STORING PERSONAL INFORMATION BE HELD LIABLE FOR IDENTITY THEFT?

With the prevalence of databases containing customers' personal information being stored in an online environment, such as occurs with cloud computing, there is an ever-present risk that data breaches of these databases may lead to identity theft.

An interesting question is to what, if any, extent businesses that store an individual's personal information should be held liable by their customers in the event of a data breach that leads to identity theft. For example, can financial institutions or other service-providers be held liable for data breaches by a third party which leads to their customers suffering loss or damage from, for example, identity theft?

In the US, some case law supports an affirmative answer. In Alabama, a bank was held liable for its negligence in failing to prevent an imposter opening up a bank account in the victim's name, which had led to the arrest of the identity theft victim for issuing worthless cheques.[15] A more recent case in New Jersey held that financial institutions have a duty to 'pursue with reasonable care their responsibility for protecting not only their own customers, but non-customers who may be victims of identity theft', but a higher appellate court later reversed this finding.[16]

While no such case has occurred in Australia, organisations can potentially be held liable in negligence for failing to take adequate precautions to prevent data breaches of their customers' personal information, which may expose their customers to suffering damage from identity theft.

However, apart from criminal sanctions discussed later, it is open to organisations to recover from fraudsters. One such case occurred when Westpac was defrauded of over $1 million by two fraudsters who had changed the addresses and telephone numbers of 27 bank customers so that debit cards, credit cards and banking details could be diverted to them and used to misappropriate customers' money. Westpac made a successful claim against the fraudsters for deceit and misleading and deceptive conduct under s42 of the *Fair Trading Act* 1987 (NSW).[17]

The consequences of identity theft for property owners are shown in the case of an absentee landlord, who alleged that one of his Perth properties was sold without his knowledge or consent as a result of identity theft.[18] The real estate agent who sold the property had received an email and phone calls from someone purporting to be the owner, saying that he needed to sell the property immediately. The estate agent acted on the scam email and put the property on the market. The agent later received documents with forged signatures and duplicates of the title deeds to both properties. The scam email is believed to have originated in Nigeria and a bank account in China was used for the sale.

Even courts are mindful of the risks of identity theft. So much so that, in September 2008, the Law Institute of Victoria made a submission to the County Court of Victoria that an identity theft prevention and anonymisation policy should be implemented in all Victorian courts.[19] The purpose of this policy is to protect members of the public who are involved in court proceedings from identity theft by avoiding the use of their unique personal identifiers in judgments and transcripts.

NEW LEGISLATIVE DEVELOPMENTS

The *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act* 2010 (Cth) (*Identity Crimes Act*) was enacted on 2 March 2011.[20] The *Identity Crimes Act* introduced amendments to the Commonwealth Criminal Code. It is similar to recent state legislation.[21] Three new offences were created as a part of the Commonwealth Criminal Code:

1. dealing in identification information;
2. possessing identification information; and
3. possessing equipment used to make identification information.

The rationale for introducing the laws relating to identity theft arose from a belief that existing offences such as theft, forgery, fraud and credit card-skimming, did not adequately cover the various forms of identity crime.[22]

The central tenet of the new identity theft offences is the definition of 'identification information', which has been defined as:

'...information, or a document, relating to a person (whether living, dead, real or fictitious) that is capable of

being used (whether alone or in conjunction with other information or documents) to identify or purportedly identify the person, including any of the following:

(a) a name or address;
(b) a date or place of birth, whether the person is married or has a de facto partner, relatives' identity or similar information;
(c) a driver's licence or driver's licence number;
(d) a passport or passport number;
(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.'[23]

Unlike the definition of personal information in the *Privacy Act* 1988 (Cth), identification information is not confined to individuals, but extends to bodies corporate. Perhaps this broad definition has arisen out of a concern that organisations may also be victims of identity theft, such as occurred with the Sydney Opera House. In 2003, a fraudulent website that was hosted and administered from overseas purported to be the official booking site for the Sydney Opera House.[24] In that case, the Australian Competition and Consumer Commission obtained declaratory relief and an injunction against Richard Chen, an individual located in the US, for contravening the consumer protection provisions of the then *Trade Practices Act* 1974 (Cth).

The prohibition against dealing in identification information is found in s372(1) of the Commonwealth Criminal Code, which states:

'A person (the first person) commits an offence if:

(a) the first person deals in identification information; and
(b) the first person intends that any person (the user) (whether or not the first person) will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of:
  (i) committing an offence; or
  (ii) facilitating the commission of an offence; and
(c) the offence referred to in paragraph (b) is an indictable offence against a law of the Commonwealth.'

The Explanatory Memorandum to the *Identity Crimes Act* provides an example of how s372(1) of the Commonwealth Criminal Code is intended to operate:

'Person A uses the identification information of a business, such as its trading name, ABN, address and financial account information to pass themselves off as the business or an authorised agent or employee of the business, with the intention of importing a tier 1 prohibited good, such as an anabolic steroid, under the *Customs Act* 1901 (Cth).'[25]

As absolute liability applies under s372.1(2) of the Commonwealth Criminal Code – the prosecution does not need to establish a fault element – with the result that the defence of mistake of fact is unavailable to an accused. So, taking the above example, even if the attempted importation was prevented by Customs, the accused would still be guilty of committing an offence under s372.1(2).

One significant benefit of the new legislation against identity theft for victims is that they can now seek a remedy against the adverse effects of identity theft by the issue of a certificate from a magistrate, which enables them to negotiate with organisations such as financial institutions to re-establish their credit rating.[26]

DOES THE NEW IDENTITY THEFT LEGISLATION ACHIEVE ITS AIMS?

The legislation against identity theft has been criticised on the grounds that it is too broad and vague.[27] Specifically, there is a concern that the offence of criminalising possession of identification information is out of step with established criminal law principles, in that a mere intent to commit or facilitate an indictable offence is sufficient to constitute an offence.[28]

As the laws are recent, there are no published decisions in this area that have considered the meaning of the new provisions. It remains to be seen how often the new laws will be used by enforcement authorities, but it is to be hoped that authorities will focus more on the act of unauthorised use of identification information, namely 'dealing', rather than 'possession'.

One such example is a recent report that the Australian >>

Federal Police has charged two men with the seizure and production of false identity documents, including one count of dealing with identification information, contrary to s192J of the *Crimes Amendment (Fraud, Identity and Forgery Offences) Act* 2009 (NSW).[29]

IS THERE A TREATY DEALING WITH ONLINE IDENTITY THEFT?

That online identity theft is on the rise is unsurprising when one considers the increasing ubiquity of the internet, the anonymity it affords and the poor IT security practices of many organisational and individual users. In addition, the nature of online identity theft is that it does not respect national boundaries. This, in turn, presents a problem for enforcing domestic laws aimed at preventing identity theft.

At present, there is no specific international treaty dealing with online identity theft, although the Convention on Cybercrime, which is the first treaty to address online crime, has been ratified by 30 countries.[30] While Australia is yet to be a party to this treaty, it is one of the few OECD countries to have enacted laws against identity theft.[31]

Clearly, the ability of countries to prosecute foreign citizens will be crucial in deterring online identity theft, and much greater international co-operation will be required to deal with this issue.

CONCLUSION

Although there have not been any cases of civil liability against companies involved in data breaches of their customer databases, it is foreseeable that courts may impose liability upon companies that fail to adequately protect their customers' personal information.

That the Commonwealth and several states have introduced specific laws against identity theft is a positive development, despite criticism about the scope of some of these laws and whether they accord with established principles for criminal law.

Given the transnational nature of online identity theft, however, much more work needs to be done on an international level to address the issue, as domestic laws provide only limited protection for online users. ■

Notes: **1** M Paphazy & A Prpich, 'Identity theft in an online environment', *Internet Law Bulletin*, Vol. 11, No. 8, December 2008. **2** ALRC Report 108, Chapter 12, *Australian Privacy Law and Practice*, at http://www.alrc.gov.au/publications/12.%20Identity%20Theft/what-identity-theft. **3** http://www.cybersmart.gov.au/Teens/Tips%20and%20advice/Identity%20theft.aspx. **4** National Privacy Principle 2 permits use and disclosure of personal information in circumstances in which an individual would reasonably expect such use or disclosure. Personal information is defined in the *Privacy Act* 1988 (Cth) as being 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'. **5** B Acoca, 'Online identity theft', *OECD Observer*, No. 268, June 2008 at http://www.oecdobserver.org/news/fullstory.php/aid/2662/Online_identity_theft.html. **6** G Brodtmann MP, in her second reading speech for the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2010* on 9 February 2011. **7** For a more detailed discussion of the other ways in which online identity theft can occur, please refer to M Paphazy & A Prpich, 'Identity theft in an online environment', *Internet Law Bulletin*, Vol. 11, No. 8, December 2008. **8** Second reading speech of M Keenan, Shadow Minister for Justice, Customs and Border Protection, for the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill* 2010, 9 February 2011. **9** www.alexa.com. **10** A Levy,' Facebook's Value Tops Amazon.com; Trails Only Google on Web', *Bloomsberg Business Week*, http://www.businessweek.com/news/2011-01-28/facebook-s-value-tops-amazon-com-trails-only-google-on-web.html; J Wortham, 'Facebook Tops 500 Million Users' 21 July 2010, *New York Times*, http://www.nytimes.com/2010/07/22/technology/22facebook.html?_r=2&partner=rss&emc=rs. **11** R Singel, 'Dating Site Imports 250,000 Facebook Profiles without Permission', *Wired*, http://www.wired.com/epicenter/2011/02/facebook-dating/; C Kell, 'Online "dating service" steals 250,000 profiles from Facebook', http://ca.news.yahoo.com/blogs/dailybrew/online-dating-steals-250-000-profiles-facebook-20110205-113925-029.html. **12** http://en.wikipedia.org/wiki/Web_scraping. **13** http://www.facebook.com/terms.php; W Hartzog, Stanford Law School at http://cyberlaw.stanford.edu/node/6613. **14** http://www.acma.gov.au/WEB/STANDARD/pc=PC_311613; http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html. **15** *Patrick v Union State Bank*, 681 So.2d 1364, 12 July 1996. **16** *Brunson v Affinity Federal Credit Union*, 402 N.J. Super. 430; 954 A.2d 550 (App. Div. 2008). **17** *Westpac Banking Corporation v Toksoz & Anor* [2010] NSWSC 1509 (23 December 2010). **18** Consumer Affairs Victoria website at http://www.consumer.vic.gov.au/CA256EB5000644CE/page/Listing-NewsAlert-2010-09-16+-+House+stolen+through+identity+theft+scam+-+Alert?OpenDocument&1=~&2=~&3=~&REFUNID=~. **19** http://www.liv.asn.au/getattachment/4dc8a6ea-d605-4d55-954b-fa1728e38ff7/Identity-theft-and-anonymisation-policy.aspx; NSW followed suit on 30 June 2010 - http://www.ipc.nsw.gov.au/lawlink/lec/ll_lec.nsf/vwFiles/Identity_theft_prevention_v_2.pdf/$file/Identity_theft_prevention_v_2.pdf. **20** *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act* 2010 (Cth). **21** *Crimes Amendment (Fraud, Identity and Forgery Offences) Act* 2009 (NSW) commenced on 22 February 2010; *Crimes Amendment (Identity Crime) Act* 2009 (Vic) commenced on 16 July 2009. **22** Explanatory Memorandum to the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act* 2010 (Cth). **23** It is worthwhile comparing the definition for 'identification information' with that of 'personal information' found in the *Privacy Act* 1988 (Cth). **24** *ACCC v Chen* [2003] FCA 897 (27 August 2003). **25** Explanatory Memorandum to the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act* 2010 (Cth). **26** Section 375 of the Commonwealth Criminal Code and s89F of the *Sentencing Act* 1991 (Vic); s309 of the *Criminal Procedure Act* 1986 (NSW); s440H of the Criminal Code (WA). **27** A Steel, 'The True Identity of Australia Identity Theft Offences: A Measured Response or an Unjustified Threat', *University of New South Wales Law Journal* (2010) 33, 503-31. **28** *Ibid* at 509; Also, see s192K of the *Crimes Act* 1900 (NSW) – a person who possesses identification information with the intention of committing, or of facilitating the commission of, an indictable offence is guilty of an offence. **29** http://www.afp.gov.au/media-centre/news/afp/2011/february/two-men-arrested-for-false-documentation.aspx; see s192J of the *Crimes Act* 1900 (NSW). – a person who deals in identification information with the intention of committing, or of facilitating the commission of, an indictable offence is guilty of an offence. **30** A Seger, 'Identity theft and the Convention on Cybercrime', *UN ISPAC Conference on the Evolving Challenge of Identity-related Crime 2007*. **31** B Acoca, *Scoping Paper on Online Identity Theft*, 2007 at http://www.oecd.org/dataoecd/35/24/40644196.pdf; *Convention on Cybercrime* at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Michael Papházy *is a corporate counsel with SingTel Optus. The views expressed are his and not necessarily those of SingTel Optus.* **PHONE** *(03) 9233 4000*
EMAIL *michael.paphazy@optusnet.com.au*