



CRIMINAL FUTURES

Robert Cornall
Secretary, Commonwealth Attorney-General's Department

*Paper presented at the
4th National Outlook Symposium on Crime in Australia,
New Crimes or New Responses
convened by the Australian Institute of Criminology
and held in Canberra 21-22 June 2001*

Introduction

Let me introduce myself. My name is Robert Cornall. I am the Secretary of the Commonwealth Attorney-General's Department in Canberra. I previously came from Melbourne where I was, at different times, the managing director of Victoria Legal Aid, the executive director of the Law Institute of Victoria and a solicitor in private practice.

Identifying myself in this way sits comfortably with this Wizard of Id cartoon (attachment A).

Alternatively, I could have said my name is Robert Cornall and my Visa card number is XXXX XXXX XXXX expiring 09/02.

Identifying myself in this way fits in with this cartoon (attachment B).

The point I am making is that we now have two identities.

The first is our traditional identity, which is still useful for social and recreational purposes.

But, for many, if not most, commercial and business transactions as well as a lot of every day activities, our electronic identity is all important and our traditional identity is irrelevant.

Identity as a Criminal Target

Until recent times, there were limited opportunities for a criminal to commit a crime by exploiting another person's identity.

But the evolution of our electronic identity has changed that situation dramatically.

Consider this not too distant future scenario:

- I leave the office at the end of the day, using my proximity card to get into the lift to the carpark in the basement of my building
- On the way home, I stop at a Coca Cola machine, ring the advertised number on my mobile phone and charge the purchase cost charged to my telephone account
- When I get home, a remote sensor opens the garage door as I enter the driveway
- I put my finger on the pad at the front door, the door opens and the burglar alarm is switched off
- The lights go on and the air conditioning turns up to my preferred temperature for that time of day
- I ring my bank, key in my account and PIN numbers and transfer funds to pay a couple of outstanding bills
- I call out to the blank screen on the wall, "Screen on", and it comes to life. Then I say "Get my mail" and my inbox appears
- There's a message from my bank and a dozen emails from companies selling goods matching my personal purchasing profile
- The bank email says: "Dear customer, Your telephone password will expire in two days. A new password will be issued following a videolink retina scan. To change your password now, click here"
- While I'm changing my password, my 3G phone beeps with a message that Maxfli golf balls are on special at only \$54 a dozen at my local golf shop.

How many of these events depended on my traditional identity? How many depended on some form of electronic recognition or an electronic device or program linked to my identity or personalised for my use?

This example illustrates another significant point.

We don't have just one electronic identity. We have separate electronic identities:

- for each bank we have an account with
- for each business we deal with electronically; and
- for every service arrangement we enter into where the billing or some other aspect of the transaction is processed on the telephone or over the Internet.

So today I want to look at some of the issues this electronic schizophrenia poses for criminal futures, because the issues of identity and technology come up in each of the three themes for this session – “crime, risk and trust”.

Is There an Identity Problem?

I'll start with the easy question first, just to get it out of the way: is there an identity problem?

Well, there is in America, according to Robert O'Harrow Jr writing in the Washington Post on 31 May 2001:

The Justice Department told Congress last week that Internet fraud, including identity theft, is one of the nation's fastest-growing white collar crimes. And John G Huse Jr, the Social Security Administration's inspector general, testified that the misuse of Social Security numbers is a 'national crisis'.

And the Sydney Morning Herald reported on 19 May 2001(page 10):

Drivers licences and birth certificates produced on home computer desktop publishing systems are contributing to a \$3.5 billion annual business in ID fraud.

We can add to those observations anecdotal evidence that financial institutions, which previously seemed content to treat fraud as an acceptable cost of doing business, appear now to be very interested in fixing this problem. This suggests that the cost of fraud is reaching profit-affecting levels that can't be ignored.

There seems to me to be several factors at work here. The first is that the myriad of electronic identities that now exist have exponentially increased the opportunity for fraud.

And those opportunities have been further enhanced because the capability of the technology has raced ahead of us without adequate protections against identity fraud being built into the system.

Crime in a High Tech World

It is often asserted that technology just provides new ways for committing old crimes.

Peter Grabosky recently wrote (The Age, 24 April 2001, Computer Section, page 1):

Many types of electronic theft are essentially traditional forms of theft in new guises.

But he added:

It is the means of committing the theft – the fact that the criminal act can occur at the speed of light, and the fact that a thief can commit the act from the other side of the world – that is without precedent.

Consider this example of a modern Internet crime.

On 27 December 2000, two defendants were sentenced to 27 months' imprisonment in California after pleading guilty to fraud related charges arising from their sending out more than 50 million spam emails fraudulently seeking money. The emails promised enormous returns for students and others who wanted to work from home in return for a \$35 "processing fee". More than 12,400 victims sent money to the defendants.

The cost of sending these 50 million emails was less than \$100. To send them by surface mail at 34 cents per envelope would have cost around \$17 million in postage alone.

(Testimony of Bruce Swartz, Deputy Assistant Attorney General, US Department of Justice - Subcommittee on Commerce Trade and Consumer Protection, 23 May 2001).

So, while there are some similarities with older scams, this crime could only have been committed on the Internet.

This is an important point. It reminds me of the first lecture I attended in Political Science II. The lecturer said we should start from the premise that the American system of politics and government was quite different to ours and then look for similarities. Thinking it was the same and looking for differences would result in incorrect and therefore misleading assumptions.

I think it is dangerous to draw too much comfort from the old crimes in new clothes approach. It is likely to create blinkered thinking and limited responses.

It would be far safer to think of them as new crimes needing new solutions.

But even if we accept the old ways to commit new crimes approach, there is no reason to think we've exhausted the problems. As computers and their uses continue to develop exponentially, so will the opportunities for crime.

Ways in Which Identity Can be Acquired

Put simply, identity can be acquired in three ways:

- a fictitious identity is created
- a real identity is acquired or borrowed; or
- an existing identity is altered.

Obviously people have used false identities before. What is new today is the ease with which fictitious identifiers can be acquired or created.

If you look up Privacyworld's Internet site, you will find step by step instructions to order an international driver's licence, an academic degree by mail or a Press Card ID.

In fact, Senator Susan M Collins, who is the Chairman of the US Senate's permanent sub-committee on investigations, said in her opening statement on 19 May 2000, that:

The high quality of the counterfeit identification documents that can be obtained through the Internet is astounding.

She went on to say that, although government agencies had progressively added security features to identification documents (such as holograms, shadow pictures and bar codes),

the Internet sites that sell fake IDs appear to have kept pace by duplicating many of these security features.

And Exploited

So how has this exploitation been applied in practice?

Take one individual example - the case in March this year of a US citizen and kitchen hand called Abraham Abdallah.

Abdallah was charged with offences derived from activities cloning the electronic identities of people such as Steven Spielberg, Ross Perot, Oprah Winfrey and Ted Turner.

He allegedly attempted to steal US\$22m from these people by counterfeiting official business documentation, using these documents to collect credit card details, determining other personal details from publicly listed sources, and utilising e-mail authorisations on their behalf to convince financial institutions to make international monetary transactions.

His activities reportedly came to notice while attempting to transfer US\$10m to Australia.

The attempted transfer was frustrated by a simple administrative difficulty - it would have resulted in the account being overdrawn.

A major concern arising from this case is the extent to which it demonstrates that Abdallah:

- was able to accumulate useful detailed personal information about prominent people; and
- was able to use this information to impersonate individuals and convince financial institutions to undertake large scale financial transactions in their name.

But the Internet makes that easy.

At the click of a mouse button and from any location in the world, I can download details of my telephone number, household address, the purchase price of property I own, maps showing where this property is situated and my email address.

I know data from these sources alone may not be enough to convince financial institutions to transfer money from bank accounts.

But it provides a good platform from which a moderately determined criminal can seek or create more intimate identity details that can be exploited for criminal purposes — as the Abdallah case demonstrates.

And, of course, misuse of identity does not stop at crimes of theft and fraud, although they are the major problem areas — the misuse also extends to new opportunities for harassment and stalking.

You may also be familiar with some of the recent cases of corporate harassment involving companies such as Microsoft, Amazon and e*Bay.

Damage from these anonymous denial-of-service attacks has been reported to be in excess of some US\$1.2b.

And identifying perpetrators - if that is possible - is a very complex and expensive exercise.

At the government level, these losses are felt in areas such as social security and Medicare fraud, failure by individuals to make their child support payments and tax avoidance.

Responses to Identity Crimes

Legislative Responses - Current and Planned

One of the challenges facing the Attorney-General's Department and law enforcement agencies is to ensure that traditional offences address new developments in technology.

One legislative response is the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*, which has just been enacted. It ensures fraud and forgery offences are adequate to encompass automatic teller machines, automated electronic funds transfers, credit cards and smart cards.

Next on the legislative agenda is the proposed *Cybercrime Bill*. This statute will, when passed, prohibit conduct that involves circumventing an electronic identification mechanism or appropriating a password or personal identification number to gain access to computer data.

It is also proposed that there be an offence with a maximum penalty of 3 years imprisonment which covers people who possess or trade in hacking programs that manipulate identity codes.

The bill will prohibit a person circumventing an electronic identification mechanism with the intention of committing a serious offence such as fraud. The maximum penalty for this new offence will be equal to the maximum penalty for the serious offence (for example, 10 years if it involved fraud).

A general offence of simply using a false identity would, of course, go too far. We would not wish to outlaw innocent activities such as, say, participating under an assumed name in an Internet chat room.

More Fundamental Responses

Now I acknowledge that creating and enforcing appropriate criminal offences is obviously necessary and important.

But it would be much better if we could address the problem of identity and fraud at its source and prevent – or at least reduce the number of - offences occurring in the first place.

This is essential because computers are all pervasive, often invisible and, according to Moore's Law, doubling in processing power every 18 months. And the same principle seems to apply to storage and memory.

One small illustration: I am quite confident my previous employer still has a record on some computer back up disk with details of each day and time I used my proximity card to get into my office at 350 Queen Street in Melbourne between 1996 and 1999 if they could be bothered to look for it.

How do we Establish Identity?

Which brings me to the crux of the matter – how do we establish identity?

You are all well aware of the 100 point identity test which applies when you want to open a new bank account. That test relies on documents like drivers' licences and birth certificates.

There are two things we can say about those sorts of documents:

- they are not intended to be used for identification purposes; and
- the process of creating or issuing them is easily abused.

I referred earlier to the American Inspector General of Social Security Administration who said SSN abuse in the United States was at crisis point.

He also said:

*...while the ability to punish identity theft is important, the ability to **prevent** it is even more critical. How do we do this? First and foremost, the time has come to put the SSN back in its box. We as a Government created the SSN, and we as a Government must control it....The SSN is a unique identifier and its ... use as an ID number by schools, hospitals and other institutions is understandable – but dangerous. Its use by Federal, State and local governments not only for taxes and other legitimate purposes, but for everything from drivers' licences to water and sewer bills, is a convenience we can no longer afford.*

Unique Identifiers

Which brings me to the topic of unique identifiers.

I note here that the Attorney-General's Department is presently undertaking a project to develop a discussion draft of a blueprint for the management of identity fraud risks.

I will not pre-empt the outcome of that research but I think one proposal that will clearly have to be discussed is the introduction of an acceptable form of unique individual identifier.

My personal view at this stage is that we need to find a way of providing people with an ironclad unique identification document surrounded with as much security and protection from copying or other abuse as modern technology can muster.

That unique identifier could then be used to establish identity for all commercial and private transactions or business relationships where it is essential to identify the participants accurately, such as when opening bank accounts or registering for government benefits and so on.

It would replace the inappropriate documents we presently use for this purpose (like drivers' licences) which fill the void and meet the ever increasing need for accurate identification documents or procedures because we have not yet developed anything better.

This unique identifier could be issued or sponsored by Government but then used for identification in all sorts of transactions, including business transactions with private sector organisations.

It would not – and would not need to be - connected or linked to any central government database for any purpose other than the issue of the identification itself.

Privacy Issues

If such a proposal was to be developed, it would obviously have to be set within extremely strict privacy guidelines.

But let's be very clear about this. Many organisations, particularly private sector organisations, hold unchecked computer records on individuals right now. Our profiles can be constructed from readily available information or accumulated from say our credit card purchases.

But we often don't know where they are kept, what's on them, who has access to the information and what they are using it for.

Look at this cartoon (attachment C). And this one (attachment D).

You can laugh, but you know it's true.

Which is why the Commonwealth Government has legislated for privacy controls on the private sector.

Deputy Federal Privacy Commissioner Timothy Pilgrim was recently reported as saying (Weekend Australian, 9 June 2001, Supplements, page 21):

In the 1980s people thought of Big Brother as the government. But now many organisations – often very small ones – are able to collect information about us. There is no doubt that in the business world, personal information is seen as a commodity and can be a valuable asset. We're trying to return control of that sort of information to the individual.

In other words, the cat's already well and truly out of the bag. Technology has run ahead of privacy controls and now we're trying to get it back under an individual's control, as Tim Pilgrim said.

Australia Card

The suggestion of an ironclad ID card may awaken memories of the Australia Card debate.

The Weekend Australian newspaper apparently thought that debate could be still alive and well when it suggested we might have to consider the *unmentionable Australia Card* in its editorial last Saturday (16 June 2001, page 18) commenting on immigration issues.

But I think the Australian got it wrong.

Look at these facts. The Australia Card debate took place in about 1985. That's 16 years ago.

Before the Internet was in common use.

Before telephone banking, EFTPOS and mobile phones.

Pretty much before Australia floated the dollar.

Before DNA and before virtually everyone had a computer, a credit account and a mobile with a plastic card, a PIN number or a password.

Before we realised we would have – by 2001 - a myriad of different electronic identities for different purposes.

Before globalisation became the buzz word of the decade.

Before we realised how exposed we all would be to identity fraud in the information age.

And, as Timothy Pilgrim says, it's turned out that there's no one Big Brother. There's no secret, central database in a basement in an unmarked building in Canberra.

The risk is from the myriad of databases being developed and maintained by just about every private, semi-government and government enterprise we deal with in our daily lives. Or the list brokers who fill any information gaps.

The secret databases are in Collins and Phillip Streets.

And that creates a real risk for all of us. It exists now. And it leaves us very exposed to identity fraud.

So, in my opinion, the Australia Card's a furphy. Let's put it to rest right now and get it behind us.

That debate has been overtaken by technology, the Internet and the way business is transacted in the 21st century. It is irrelevant. It's a relic of the 80s ready for preservation by the National Trust.

The key objective now is to control the information that has already been gathered – and is increasing every day - and the uses to which it is put.

But given the way databases have in fact developed and the way stored information is used, it is clear that Government can only address this problem of identity fraud with the close and active cooperation of the private sector.

Technology Creates the Problems But Technology Can Supply the Answers

The final point I want to make is that technology creates many of these problems but technology can also supply the answers.

I think it is essential that our response to issues like identity fraud should be at two levels.

One is a technological response: how do we apply technology to prevent or defeat the problem?

Look at these simple examples:

- PIN numbers for car radios needed when the battery is disconnected
- Global positioning systems fitted in new cars to locate them if they are stolen
- Drink drivers – alcohol ignition interlocks – presently under consideration in Victoria (see advertisement Herald Sun 15 June 2001, page 32)
- Recording your mobile international mobile equipment identity, which will allow police to obtain the identity of the phone's current user from the mobile phone carrier - press *#06# to find your phone's IMEI (see Crime and Justice Bulletin, Number 56, March 2001 published by the NSW Bureau of Crime Statistics and Research)
- Can we develop some form of PIN number protection for credit cards when they are used over the phone or on printed forms? (How exposed are we to fraud leaving our credit card number and expiry all over the place?)

You may say you've heard all these ideas before.

I don't make any claim for originality but I do say that ideas are easy to come by. The hard part is developing a good idea into an accepted policy and implementing it in practice. That's where the really hard slog is.

The second is the legislative response to outlaw or penalise crimes we haven't yet found a way to prevent.

Conclusion

So in conclusion, I want to summarise the points I have made today.

1. We now have two types of identity: our traditional identity and our electronic identity or, more likely, identities.
2. This duplication of identity has created much greater opportunity for identity fraud.
3. We need to find better solutions to the problem of establishing identity and we should be able to do so while preserving – or even enhancing – individual privacy.
4. We need to accept and act on the basis that, while technology creates the problem, it can also provide the answer.
5. So one level of response should be to look for a technological solution to prevent the problem occurring.
6. But that can only be done by Government and business in partnership. Government alone can't do it because it doesn't control either the technology or, in most cases, the databases.
7. The other - and separate – level of response is to keep our criminal law up to date with developments in technology that either facilitate innovative crimes or put a new spin on old ones.