



**Australian
Privacy
Foundation**

February 2005

Review of the Photo Card Bill 2004

Introduction – what this document is for

This paper sets out the Australian Privacy Foundation's analysis of the *Photo Card Bill 2004 (NSW)*, including the features of most concern in terms of risks to individual privacy and overall security.

An appendix to this paper also sets out a number of questions we have about the Bill, for which we seek answers from the Minister for Roads, the Hon Michael Costa MLC.

Overview of our concerns

We do not disagree with the Government's legitimate objective of assisting those members of the community who face some difficulty in life without one of the more common forms of photo ID, such as drivers' licences.

However we do not believe the model proposed in the Photo Card Bill will achieve those objectives.

Furthermore the Bill, in its current form, poses not only privacy risks for individual Photo Card holders (*and* people who hold a driver's licence), but security and corruption risks for the RTA, as well as possibly hampering law enforcement efforts to tackle identity theft and fraud. This is because the Bill introduces a centralised identity management system.

The good news is that there are other options, which are outlined below.

Identity cards: what's in a name?

Photo Card or identity card?

Whatever you call it, the card proposed in the Bill (a Photo Card), is intended to work as an identity card.

The Explanatory Notes to the Bill state:

"The Photo Card can be used as evidence of the age and identity of a person".

Unlike driver's licences, which are primarily intended to establish one's ability to drive but have evolved as a defacto proof of identity, the Photo Card is designed with the primary intention of being proof of identity and age.

Although there is an existing 'proof of age' card available to 18-25 year olds in NSW, general-purpose identity cards such as that proposed in this Bill have not been issued in Australia other than during World War II. For that reason we demand a high degree of scrutiny of the potential privacy and security impacts of this proposal.

Access to services – will the basic problem be solved?

The Government has stated:

"The card ... will help those in the community who have a need for a photo card ... The card will provide New South Wales residents who do not hold a driver's licence with a document that will assist them to establish their entitlement to rights and privileges in the community."¹

However it would seem that it is not so much "entitlement to rights and privileges" that are at issue, but access to basic goods and services, that should be available to all.

It appears to be an increasing trend that people are requested to provide some photographic proof of their identity before they can access goods and services, where previously routine transactions did not require such proof. Examples include posting a parcel overseas or taking a domestic flight, buying a mobile phone or renting a video, and entering a licensed club or pub.

This poses a difficulty for people who do not possess common photographic documents such as a driver's licence or a passport. It is this difficulty which the Photo Card Bill seeks to address.

However we are concerned that the introduction of a Photo Card, if in the form proposed in this Bill, will exacerbate this situation for many people.

The intention of the Photo Card is that it be available to all people who do not have a driver's licence – and explicitly *not* available to people who *do* have a driver's licence. By definition then, the Photo Card is intended to "fill the gaps" between existing forms of ID.

What is unique about this proposal is that will create a uniform identity management system, run by one government agency, using one database designed to capture details on all NSW residents – both drivers and non-drivers². (This is a similar centralised identity management model to that which was proposed by way of the highly unpopular *Australia Card*, which was withdrawn in 1987.)

The very creation of this new form of ID strips away from people the ability to be anonymous. There will no longer be a perfectly valid explanation ("I don't drive") for why a person does not have a photographic identification document handy at all times.

¹ Second reading speech, NSW Legislative Assembly, 8 December 2004.

² Clause 14 of the Bill allows the RTA to store information about Photo Card holders on the same database as that used for drivers' licences.

Overseas experience tells us what happens next³. Providers of goods and services know that their clients or customers no longer have a 'real' excuse for not having photo ID, and so they will start demanding photo ID in more and more routine transactions.

This self-perpetuating cycle will create a new class of disadvantaged people – those who decide not to purchase a Photo Card, or who cannot obtain a Photo Card according to the whims of the RTA (see below under 'Identity denial'). This new socially-disadvantaged class will include immigrants from countries with oppressive regimes who are naturally distrustful of any form of government intrusion, people with religious or cultural objections to ID cards or having their photographs taken, individuals who have particular security reasons to prefer anonymity, and those who simply place a high value on their personal privacy.

And then the simple act of posting a gift to an overseas relative will become a "privilege", denied to some, instead of a joy for all.

We will discover that photo ID from the RTA, in whatever form, becomes a 'licence to live'.

Identity denial as social punishment

An even more disturbing aspect of the Bill is the ability of the RTA to deny a Photo Card to someone who wants a card, even if they meet the primary eligibility criteria of being residents over 16 who do not have a current driver's licence⁴.

This means some of the people for whom the Photo Card is allegedly intended – people who wish to prove their identity to third parties but cannot use a driver's licence to do so – can be denied the benefits that the Photo Card is intended to bring. This creates a whole new regime of punishment, determined not by the courts but by the RTA.

It would appear the driver's licence model was taken and simply applied without thinking to the proposal for an identity card for non-drivers⁵. After all, a driver's licence is not intended as an identity document, and thus works on a different set of rules and assumptions: it is a certificate establishing one's credentials (this person has passed certain tests), it is a permissive document (this person is allowed to drive on public roads), and it is a conditional document (this permission may be withdrawn if this person disobeys the road rules). Driving is a privilege and there are public dangers that go with driving, for which people need to be held accountable. This is not true of identity cards: one's identity is not conditional.

Yet the Bill establishes the RTA as the arbiter of whether or not a person can live with ease in their community, or instead be ostracised for their (real or perceived) short-comings. How should such people answer the question "*Why can't you just get a Photo Card?*"?

³ For example when a social insurance number (SIN) was introduced in Canada for a single purpose, it was quickly adopted by businesses who demanded to sight or copy customers' SIN card for even straight-forward transactions; see Robert Marleau, Interim Privacy Commissioner of Canada, *Why We Should Resist a National ID Card for Canada*, Submission of the Office of the Privacy Commissioner of Canada to the Standing Committee on Citizenship and Immigration, 18 September 2003.

⁴ Clause 6 of the Bill says a person who has lost custody of their driver's licence (such as through suspension of their licence for a driving offence which requires surrendering the physical card) cannot obtain a Photo Card. Clause 7 of the Bill allows the RTA to refuse to issue a Photo Card to people convicted of various offences, or on other, unspecified grounds.

⁵ In addition to the ability of the RTA to deny someone a Photo Card, see also clauses 12, 14 and 16, which set out a range of powers and penalties to regulate Photo Card holders once they have a Card, and clause 19, which allows the RTA to exchange information about Photo Card holders with interstate driver licensing authorities.

Why should a person who has lost their driver's licence because of their driving conduct also then be denied the opportunity to buy a mobile phone, take a flight or post a parcel overseas?

Why should a person who has been convicted of a criminal offence be denied the opportunity to rent a video, borrow a library book, or go to an RSL club?

The denial of a person's identity by the central identity-issuing agency, or at least of the rights that a 'normal' person enjoys, is a spectre that was imagined by George Orwell in 1984, in the form of an 'unperson'. This is 'Big Brother' behaviour in the extreme.

Voluntary systems mean no privacy risks : true or false?

The fact that the Card is "voluntary" is the most common answer we hear when we say we have privacy concerns about the Bill : "if you don't like the privacy risks, don't buy the Card" is what we're told.

Frankly, we don't think that's good enough.

First, because people who choose to buy a Photo Card should have their privacy respected and protected. Some of the privacy and security risks for Card holders (if the current model goes ahead) are outlined below.

And second, because we're not convinced that the Card is really voluntary anyway.

Compulsory in effect, if not in law

It is true that the Bill does not make the Photo Card mandatory for all non-drivers in NSW.

But it may become compulsory by social sanction, if not by law. Even a nominally 'voluntary' system can have a significant coercive element.

Those people who decide not to possess either a driver's licence or Photo Card will likely find themselves increasingly frustrated in their attempts to access government services or interact with a variety of businesses. Eventually, even people with strong objections to holding photo ID will be forced by circumstance to give in. And so a 'voluntary' system becomes compulsory by force of social and economic sanction, rather than by force of law. The effect is pretty much the same.

In any case, the Bill proposes a range of powers and penalties to regulate Photo Card holders once they have a Card, which are inconsistent with the notion of the Card being 'voluntary'⁶.

⁶ Clause 12 of the Bill requires people to notify the RTA not only if their Photo Card is lost or stolen, but also if it is damaged or destroyed. This should not be necessary if the Card is voluntary, as only a lost or stolen card could possibly be re-used fraudulently by another person. Furthermore clause 14 of the Bill requires the RTA to maintain a database of details about Card holders, including their residential address and address for service of notices. It also allows regulations to be made that would empower the RTA to require Card holders to notify the RTA of any change of address. And clause 16 allows the RTA to insist that a Card holder turn up at an RTA office and show them particular paperwork, to prove their current address. If the person refuses, they can be fined \$2,200. None of these powers should be necessary for a 'voluntary' card, and are particularly harsh for disadvantaged people such as the homeless.

Proposal establishes a unique ‘total population’ database

As mentioned already, the Photo Card is intended to “fill the gaps” between existing forms of ID, so that every resident in NSW over the age of 16 will be eligible for either (but not both) a driver’s licence or a Photo Card, both managed by the RTA, through the same database⁷.

What is therefore of most concern about this proposal is that it will create, for the first time in Australia, a uniform identity management system, run by one government agency, using one database designed to capture details on all NSW residents over the age of 16.

This is very similar to the type of centralised identity management model which was proposed for *Australia Card*, which was withdrawn in 1987 because of its controversial and highly unpopular status.

Having virtually all residents of a State listed on the one database – including their name, gender, date of birth, current address and photographic image – is unprecedented in Australia’s history.

It means that when issued by the same agency to two mutually exclusive populations which together make a whole (drivers + non-drivers = everyone), the two cards (drivers’ licences and Photo Cards) together create a near-universal identity card, and a unique identifier – the card number. And that means that the database supporting the system becomes a ‘total population’ identity database.

This has enormous privacy implications for existing driver’s licence holders as well as people holding a Photo Card.

It means the personal information held on Photos Cards and drivers’ licences, and stored on the RTA’s database, becomes much more valuable than just the current drivers’ licences and database of drivers as stand-alone sources of information.

This has a number of side effects:

- more pressure to collect more and more information about people, not just about their age and identity
- more pressure to allow sharing of information across government agencies
- more incentive for businesses to use data from the card to link transactions and conduct ‘profiling’ of customers
- more incentive for organised criminals to access the database to create fake identities, or steal real ones
- more incentive for unauthorised use and disclosure – a ‘honey-pot’ database for locating people

⁷ Clause 14 of the Bill allows the RTA to store information about Photo Card holders on the same database as that used for driver licences.

Effect 1 : Collecting more information than necessary

'Function creep' is the process by which a database of information collected for one purpose is later used for another purpose, or many other purposes. Privacy laws are supposed to protect against this process of what is known as 'secondary use'.

(Indeed allowing the agency responsible for "roads and traffic" to branch out into other activities relating to people who by definition don't drive on roads or create traffic is itself an example of 'function creep'.)

The pressure to allow function creep is often cast in economic or efficiency terms: allowing multiple uses for a system can justify spreading the budget burden across a number of government agencies, and can make a project appear economically viable where a stand-alone system would not.

It looks like the RTA has already given in to either temptation or pressure to allow function creep. The Bill allows the RTA to include *any* information about Card holders, for *any* purpose, on their database⁸.

The Government has also indicated that the Bill enables the RTA to "adapt the photo card to incorporate future developments ...which ... may include the use of biometric indicators"⁹.

This open-ended nature of the Bill means that the RTA could for example start collecting information about a Card holder's citizenship or immigration status, their health information, their pensioner status ... where would it stop? It would even allow the RTA to collect people's fingerprints or DNA.

The Bill should instead be limited to only allowing the RTA to collect or store such information as is strictly necessary to establish age and/or identity.

In particular, the use of biometrics would be a major step towards a new form of surveillance for the whole population. We believe the Bill should instead prohibit the inclusion of any new information, including biometric information, without a full Privacy Impact Assessment and a statutory public consultation period.

Effect 2 : Sharing more information than necessary

Function creep can occur not only in relation to how much information is collected, but in expanding the rules about who has access to that information. Again the argument is usually cast in economic or efficiency terms: since the data already exists, we can avoid duplication / cost / inefficiency by allowing other government agencies access to the central database.

Again it looks like the RTA has already given in to either temptation or pressure to allow function creep in terms of sharing the data. The Bill allows the RTA to disclose photographs, or any other information about Card holders held on their database, to:

- the NSW Sheriff (to recover fines),
- NSW Police (for any reason),
- driver licensing authorities in other States and Territories (for any reason), and
- any other person or organisation, so long as it is "as provided under any other law", or "in accordance with the regulations".¹⁰

⁸ See clause 14 of the Bill.

⁹ Second reading speech, NSW Legislative Assembly, 8 December 2004.

¹⁰ See clause 19 of the Bill.

It may be fair enough that police should be able to have access to information in the database where they reasonably need the information to help prevent, solve or prosecute a crime, or find or identify a missing person. So why doesn't the Bill just say that? We don't want a situation where any police officer or civilian employee of the Police can access the database without a legitimate reason.

The provision for interstate government agencies to have access to the information is clearly ridiculous. Why would driver licensing authorities outside NSW need to know about people who, by definition, are *not* licensed to drive?

And the "any other law" provision is so wide you could drive a truck through it. It is easy to imagine some other organisations that would love to get access to information on the database: the Tax Office, Centrelink and Immigration would no doubt like to access what will effectively be a 'total population' register.

In fact the Tax Office, Centrelink and Immigration already have the power to demand State government agencies like the RTA hand over any personal information they hold¹¹.

The RTA also already has legal authority to provide information to the Australian Electoral Commission about drivers from its drivers' licence database¹² – will this apply to non-drivers too?

Who would be next in line to seek access to the database?

We believe that if the RTA is to be allowed to disclose Card holders' photographs and other personal information to other organisations, all such organisations should be named in the Bill with reasons given to Parliament to debate, and there should be limitations set by Parliament in the Bill itself.

Effect 3 : Tracking and profiling

The creation of a 'total population' database means a unique identification number – the card number on a person's driver's licence or Photo Card. Creating a 'unique identifier' means governments and businesses can easily and confidently link information about people, and thus build up profiles of their activity.

So while we might not mind showing a 'proof of identity' card each time we board a plane, mail a parcel overseas, enter a pub or open a bank account, the idea that all those aspects of our daily lives might be tracked, linked and profiled - and used to make decisions about us - is far more disturbing. Anonymity in our daily lives is necessary if we are to protect freedom of speech, expression and association.

Robert Marleau, a former Privacy Commissioner of Canada, sums up the issue well:

Identification cards allow us to be identified even in situations where we have every right to remain anonymous. Unless technological limits are built into them and strict controls placed on their use, they inevitably reveal more information about us than is required simply to establish our identity or authorization in a particular situation. And without technical limitations

¹¹ See for example s.141 of the Taxation Administration Act 1953; ss.192 and 198 of the Social Security (Administration) Act 1999; and s.18 of the Migration Act 1953.

¹² See clause 25 of the Road Transport (Driver Licensing) Regulation 1999.

and strict controls on their use, they are a powerful tool to link together our various activities and produce profiles of our lives.¹³

The Bill doesn't set any limits on what information about a person will be stored on the Card, and in what form. Current technologies include magnetic stripes or 'smart card' microchips. We don't know whether any security measures will be taken to prevent information being captured electronically from the Card by third party users, such as a pub using a magnetic stripe reader to download a person's details.

We suggest it should be made illegal, and as technologically difficult as possible, for a third party to copy information from the card in any way. In particular, the card number should be prohibited from being used as a unique identifier through which to link customer information. This is already a feature of privacy laws around Australia, except for the one that now regulates the RTA¹⁴.

Effect 4 : Risk of greater identity fraud and identity theft

Identity fraud and identity theft not only facilitate a wide spectrum of unlawful activity (from under-age drinking to welfare fraud, from money laundering to terrorism), but in the case of identity theft, present a very serious privacy invasion for the person targeted. As privacy advocates we therefore take this issue very seriously - we too want systems that will prevent identity theft and fraud.

However our concern is to ensure that such projects are measured - that they will meet their objectives of reducing opportunities for identity theft, and not exacerbate the problem; that they present a proportionate response to the problem; and that any less privacy-invasive alternatives are preferred.

The Photo Card Bill allows the RTA to hold personal information about non-drivers on the same database as personal information about drivers. The Australian Privacy Foundation is concerned that this centralised database model of identity management presents a major security risk, and could hamper, rather than enhance, law enforcement efforts to tackle identity-related crime.

Systems which rely on centralised identity management (such as a central database holding lots of information about each person) can actually *increase* the risk of identity theft and fraud, in two ways.

First, a central database model makes it easier for the organised criminal or terrorist to steal a real identity or create a new fake one - they only have to bribe one person, or hack into one system, or forge one document, or fool one agency, instead of many¹⁵.

¹³ Robert Marleau, Interim Privacy Commissioner of Canada, *Why We Should Resist a National ID Card for Canada*, Submission of the Office of the Privacy Commissioner of Canada to the Standing Committee on Citizenship and Immigration, 18 September 2003.

¹⁴ The Federal Privacy Act 1988 which covers Federal government and large businesses, the Victorian Information Privacy Act 2000 and the Northern Territory Information Act 2002 which regulate their governments' activities, and even the NSW Health Records and Information Privacy Act 2002 which regulates health service providers and holders of health information, all contain provisions limiting the use of 'unique identifiers'. However the NSW Privacy and Personal Information Protection Act 1998, which regulates NSW public sector agencies, does not.

¹⁵ In issuing either Photo Cards or drivers' licences, the RTA must rely on 'foundation documents' such as birth certificates to establish identity in the first place. These documents are often more easily forged or illegally obtained, then used to gain a genuine driver's licence in a fake or stolen name. For example, seven of the hijackers in the 11 September 2001 attacks in America had genuine driver's

Second, the greater the perceived value of a Photo Card in proving identity, the greater is its value to organised criminals. Individuals, businesses and government agencies will come to rely on the driver's licence / Photo Card alternative as a single 'proof of identity'. This false sense of security allows reliance on a piece of plastic as evidence of a person's honest intentions, instead of exercising common sense or precaution. That is, by creating a single trusted identity document, the government also creates a new opportunity for organised criminals and terrorists to fool a complacent public.

This model also makes the repercussions of identity theft worse for the victim, as the degree of privacy invasion is greater, and the ability for a person to remedy a theft of their identity is more complex¹⁶.

Centralising identity management increases both the risk of identity theft, and the degree of harm suffered by the victim when it occurs. For these reasons the Federal Australian Government and the United States Government have recognised the security flaws in creating or relying on a single identity document or single database¹⁷. Why doesn't the RTA?

Effect 5 : Risk of unauthorised use or disclosure

A 'total population' database, which contains everyone's current residential address details¹⁸, is a tempting honey-pot for anyone who wants to locate anybody else: jealous or violent ex-partners, celebrity stalkers, and people intent on harassment or harm against former associates, protected witnesses, police officers, judges, prison warders, lottery winners, politicians, and so on.

So every person living in NSW would be locatable by breaking into or bribing one's way into the RTA's database.

In 1992 the NSW Independent Commission Against Corruption (ICAC) finalised its investigation into the unauthorised release of, and corrupt trade in, government information¹⁹. The RTA was one of the organisations found to be a rich source of personal information, provided through unauthorised disclosures. The value of its database of drivers (in particular, their current home addresses), and the extensive size of its workforce with access to the database, made the RTA extremely vulnerable to corruption.

licences, which they obtained using fake foundation documents, purchased for between US\$50 and \$100; see Matthew Barakat, "Hijackers' bogus identification cards prompt scrutiny of state licensing rules", *San Francisco Chronicle*, 9 October 2001, available at www.sfgate.com. An American report suggests birth certificates are the main source of identity fraud; see *Birth Certificate Fraud*, Office of the Inspector General, Department of Health and Human Services, September 2000, available at www.oig.hhs.gov.

¹⁶ The inclusion of biometric data can make this process even more difficult for the innocent victim of identity theft; once a biometric other than theirs is associated with their data in a trusted database (whether through error or fraud), it is extremely difficult for the person to prove otherwise.

¹⁷ See Rachel Lebihan, "Privacy fears rule out central database", *Australian Financial Review*, 31 January 2005, p.17; and a discussion of the recommendations of the US Federal Advisory Committee on False Identification in *Your Papers Please: From the State drivers license to a national identification system*, Electronic Privacy Information Center, February 2002, available at www.epic.org

¹⁸ Clauses 14 and 16 of the Bill make it mandatory for card holders to keep the RTA informed of current residential address – not even a post office box will be sufficient.

¹⁹ Ian Temby QC Commissioner, Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information*, August 1992; see especially Chapter 12 : The right to privacy.

However unauthorised disclosure with serious repercussions does not always involve activity as dramatic as bribery or computer hacking²⁰. In some cases one only needs to ‘sweet talk’ or fool a clerk to gain access to information. In a recent example, a woman gained information from the RTA about her ex-partner, including his new home address, which he had explicitly told the RTA to keep confidential from her²¹. She had simply presented a copy of a third-party insurance renewal form for his car, and asked for the car registration forms to be re-issued to her. The forms showed his new address.

Having privacy laws which can compensate a person for a breach is not enough. The risk should be avoided in the first place.

Personal security risks for Card holders

Even if the Photo Card proposal did not involve a ‘total population’ database run by the RTA, there would remain some issues of personal security for card holders, which could be addressed using better alternatives.

The Bill allows the RTA to determine what information will be shown on the Card²². It does not set any limitations or provide any details about what information this might be.

However the Photo Card is only intended for, and may only be requested by third party users where it is reasonable to request, proof of age or identity²³. A current address is not a piece of information connected to proving a person’s age or identity to a third party such as a pub or an airline. However having a person’s home address on a printed card can have personal security risks for that person.

Perhaps it is fair enough that if I want to enter a pub, or claim a senior’s discount, I should show proof of my age. But why should a bouncer or shop clerk also be able to see where I live, or indeed my name?

Young women who are at greater risk of harassment, and elderly people who are at greater risk of burglary, might be most concerned to protect their personal security by not revealing their home address²⁴. But they will not be the only ones; as noted above, victims of domestic violence, celebrities at risk of stalkers, and people in sometimes dangerous professions such as police officers or judges, may also prefer to keep their home address private.

We believe a Photo Card holder should be able to choose what information is to be shown on the Card to suit *their* purposes – not the purposes of government agencies, businesses or criminals. The privacy and security of Photo Card holders is best protected by multiple documents, each serving limited purposes.

²⁰ Consider example a recent Victorian example, *Complainant B v Statutory Entity [2003] VPrivCmr 2*. In that matter \$25,000 compensation was paid to a victim of domestic violence who went into hiding after her new name and address (which even her parents didn’t know) were disclosed by a government agency to her violent ex-husband, despite specific assurances.

²¹ See *NR and NP v Roads and Traffic Authority [2004] NSWADT 276*, available at www.lawlink.nsw.gov.au/adtjudgments. In this case the RTA was found in breach of the non-disclosure provisions of the Privacy and Personal Information Protection Act 1998; as at the date of writing no remedy has yet been determined for the breach.

²² See clause 10 of the Bill.

²³ See clause 30 of the Bill.

²⁴ For example an 18 year old woman who only wants a card to prove her age, so she may go to a pub or nightclub, might choose to reveal her photo and age to a nightclub bouncer, but not her name or home address.

Indeed we believe that a person should be allowed to hold multiple cards, and thus multiple identifiers, so long as the issuing agency knows they belong to the one person.

The good news : there are better alternatives

Why should the Photo Card system be built to suit the RTA instead of the people who asked for it?

We believe that we should be able to deliver what non-driving members of the community want, without compromising their (or anybody else's) privacy or security.

Following discussion with key community groups who are seeking some form of photo ID for non-drivers²⁵, the Australian Privacy Foundation has developed an alternative proposal, which seeks to meet the community's needs without compromising their privacy or security.

Here's what we've come up with – and what we're asking the Government to deliver:

- a photographic card where the card holder can choose how much, or how little, of their personal information will be stored or displayed on the card
- there be no requirement to provide or maintain current address with the card-issuing agency
- a person may choose to hold more than one card – that is, different cards for different purposes²⁶
- photo cards to be issued by a separate agency to the RTA
- photo cards to use a different numbering system to drivers' licences
- the database supporting the range of photo cards not to be shared or linked in any way to the driver's licence database held by the RTA
- the law to explicitly limit the collection and use of data to its original purpose
- the law to have explicit prohibitions on the sharing of information from the database other than with police for law enforcement purposes

²⁵ We have met with NCOSS & Combined Pensioners & Superannuants Association of NSW Inc (CPSA) on this issue.

²⁶ For example, an 18 year old woman may like to have a 'proof of age' card just showing photo and age bracket ('over 18') for use at the pub, but also a separate driver's licence for use when driving. A 35 year old man may choose to have a 'proof of identity' card just showing photo and name, to use when flying interstate or opening a bank account. A 72 year old woman may choose to have a 'proof of age' card, showing just photo and age bracket ('over 65') in order to claim some seniors' discounts. And a 55 year old man may choose to have a card which shows everything he might need in one place – photo, name, date of birth, home address and signature.