Australian Government

Office of the Privacy Commissioner

PRIVATE SECTOR INFORMATION SHEET 20 – *Scanning 'Proof of Identity' Documents*

Key Messages

Good privacy practices are good for business. The Office of the Privacy Commissioner (the Office) is aware that with the adoption of new technologies by many businesses, the practice of scanning 'proof of identity' documents is becoming more common. This practice can, however, create significant privacy risks and could undermine customers' trust in the business. In some cases, customers may choose not to do business with that organisation.

This Office's *Community Attitudes to Privacy 2007* survey found only 18% of individuals surveyed felt it was acceptable for identification documents to be copied in order to obtain entry into licensed premises.

A business may only scan customers' identity documents if it is necessary for its functions or activities. In the first instance businesses should consider whether identification is required and, if so, whether simply sighting a 'proof of identity' document without scanning it would be sufficient.

Businesses that do seek to use scanning technology must make sure they comply with the National Privacy Principles in the Privacy Act which regulate the collection and handling of personal information by businesses. In general, if you scan customers' identity documents, the Privacy Act requires that, among other things, you:

- collect only necessary personal information;
- give customers information about why you are collecting their personal information and how it will be handled;
- only use or disclose the personal information for the purpose of the collection, unless an exception applies;
- only retain the scanned personal information for as long as necessary, consistent with the collection purpose;
- store the personal information securely and allow access to it by the individual if requested.

Businesses may be able to have greater confidence about meeting their obligations under the Privacy Act by getting the express consent of customers before scanning identity documents. Seeking consent is also good privacy practice and likely to promote trust between the customer and business.

It is important to note that if you collect health or other types of sensitive personal information by scanning, the Privacy Act says that you *must* get consent.

The Privacy Act gives individuals the right to complain if they think their personal information has been mishandled and the Office can investigate these matters. For more information please see our website at www.privacy.gov.au/privacy_rights/complaints.

Background

Who is this information sheet for?

This information sheet is for all organisations in the private sector that are covered by the Commonwealth *Privacy Act 1988* (the Privacy Act). These organisations must comply with the ten National Privacy Principles (NPPs) in the Privacy Act when handling personal information. In particular, this information sheet is directed to organisations using scanning devices, or contemplating the use of scanning devices, to collect personal information.

Section 6C of the Privacy Act sets out the types of entities that are considered to be an organisation. Notably, there is an exemption for some small businesses. The general definition of a small business operator for the purposes of the Privacy Act is a business with an annual turnover of $3 million or less. Small businesses that are not exempt include those that are related to a business covered by the Privacy Act, trade in personal information or provide a health service.

If you are a small business and you are considering trading the personal information collected through scanning technology, for example, by selling it, this may mean you will be subject to the Privacy Act. For more information about coverage and exemptions from the NPPs please see our website at www.privacy.gov.au/publications/IS12_01.html.

What is this information sheet about?

This information sheet gives guidance to organisations on how the NPPs in the Privacy Act apply to personal information collected using scanning technology.

The Office is aware of the increasing use of scanning devices and has received enquiries and complaints about organisations using scanning technology to collect personal information, particularly from documents such as driver's licences, commonly referred to as 'proof of identity' or ID documents.

These enquiries and complaints reflect concern about not only the amount of personal information being collected, but also the ease with which that electronically stored personal information can then be inappropriately copied, searched, used and disclosed. More simply, personal information recorded on paper files is much harder to manipulate than in electronic form. Scanning increases the risk that the personal information collected could be used for improper purposes.

Why is scanning proof of identity documents a privacy concern?

Once personal information has been collected by scanning, it becomes digitised and has the potential to be used or disclosed for many other purposes such as direct marketing or the creation of customer databases. Individuals may be concerned that scanned and electronically stored personal information can be matched to personal information held by other organisations. This can create a detailed picture of how they go about their day to day activities.

With the rise of identity crime, there are also legitimate community concerns about possible misuse of personal information, especially with regard to identity information contained on driver's licences and other proof of identity documents.

Individuals are also concerned that the stored personal information could be compromised through hacking, computer theft or other inappropriate access. Those who steal the personal information may be able to do significant damage to the individual, whether by committing financial, credit card or identity fraud.

Good privacy practices are good for business. Avoiding practices that might create privacy risks, such as routinely or unnecessarily scanning ID, will help promote consumer trust and confidence in the business. It is worth noting that only 18% of individuals feel that it is acceptable for identification documents to be copied in order to obtain entry into licensed premises.[1]

[1] See *Community Attitudes to Privacy 2007* on our website at www.privacy.gov.au/publications/rcommunity07.pdf.

What do the National Privacy Principles generally do?

The NPPs give individuals a certain amount of control over their personal information by limiting the circumstances in which organisations can collect, use and disclose personal information.

The NPPs require that organisations tell individuals when their personal information has been collected, why it is being collected, what will happen to the information after it has been collected and allow the individual access to the personal information that has been collected. The NPPs also require that organisations take steps to secure the personal information it collects and securely destroy it if it is no longer required.

Below are some comments on how a range of NPP requirements relate to scanning proof of identity documents:

NPP 8 Anonymity

Do individuals have a right to remain anonymous?

Yes, NPP 8 requires that wherever it is lawful and practicable, organisations must give people the option to transact anonymously (NPP 8).

Anonymity is an important element of privacy. However, in some cases, it will not be practicable to do business anonymously, such as where an individual's personal information is fundamental to the transaction. In others cases there will be legal obligations that authorise or require the individual to be identified or to show proof of their age, for example, government regulation such as a licensing law.

However, even if an organisation has an obligation to establish proof of identity or age it is not necessarily the case that scanning that information is required. An organisation would need to be able to explain why simply sighting the document without scanning would not be sufficient.

The primary question for an organisation in deciding whether to collect personal information by scanning or other means is, 'Is it lawful and practicable to transact with an individual without collecting their personal information?' In some cases, a law may require that an individual be identified such as with some licensing laws or laws intended to prevent money laundering (though such laws may only require that information be sighted, not copied and retained). If no such laws apply, then it would be lawful for the customer to transact anonymously. An organisation would then need to consider whether it is also practicable. For example, knowing the name and contact details of an individual may be essential to the transaction being entered into, and the organisation would therefore be able to collect necessary personal information.

However, if it is both lawful and practicable for the individual to transact anonymously, then the organisation should not collect the personal information. If not, then the organisation may collect the personal information as long as it complies with the following NPPs.

NPP 1 Collection

What is required when individuals' personal information is collected under National Privacy Principle 1.1?

NPP 1.1 requires that organisations must only collect personal information that is necessary for one or more of its functions or activities.

Any organisation that collects personal information by scanning, particularly proof of identity documents, should consider whether scanning and electronically storing the personal information is necessary for one of its specific functions or activities, or whether simply sighting the proof of identity documents would be sufficient in the circumstances.

Organisations need to be clear as to what *actual* personal information on proof of identity documents might be necessary to collect, if any, for the organisation's particular functions or activities.

In addition, organisations may be able to have greater confidence about meeting their obligations under the Privacy Act by getting the express consent of customers before scanning identity documents. Seeking consent is also good privacy practice and likely to promote trust between the customer and organisation.

What is 'sensitive' personal information and how does it affect the collection of proof of identity documents?

The Privacy Act recognises that some personal information, such as health related information and information about racial and ethnic origin, is considered 'sensitive' and affords the management of this personal information a higher level of protection. Health information relates not only to the individual's existing health matters, but also includes information about the individual's wishes concerning future health services. For example, the organ donor information recorded on some driver's licences is sensitive personal information.

Under NPP 10 an organisation is required to obtain the individual's consent to collect sensitive personal information, or to ensure that one of the other specified exceptions in NPP 10 applies when collecting the personal information. For more information about the collection of sensitive personal information please see our website at www.privacy.gov.au/health/guidelines/index.html .

How does National Privacy Principle 1.2 impact the way individuals' personal information is collected?

NPP 1.2 requires that the collection of personal information should be conducted by lawful and fair means and not in an unreasonably intrusive way. This means that the scanning should not be conducted without the knowledge of the individual and should not be conducted using covert means. It should be clear from the outset that the personal information will be collected using scanning devices and those devices should be visible to the individual while the personal information is being scanned.

What does National Privacy Principle 1.3 require that individuals be told about the collection of their personal information?

NPP 1.3 requires that organisations provide the customer with certain information at the time of collection, or as soon as practicable after collection.

Organisations that are currently collecting or considering collecting personal information by scanning should be aware that individuals may express concerns about the possible loss of control of their personal information once it has been scanned. For these reasons it is important to provide clear and detailed information to individuals at the time of the collection. This information should include:

- the purpose for which the personal information is being collected;
- the intended recipients of the personal information;
- any law that requires that the personal information be collected;
- the consequences of not providing the personal information;
- that the individual can gain access to the personal information; and
- the name of the organisation collecting the personal information and how to contact it.

If this information is not provided at the time of collection, or as soon as practicable after collection, it is possible that the collection will breach NPP 1.3. Note that organisations have an obligation to provide this kind of information in their privacy policy (see discussion about NPP 5 below).

NPP 2 Use and Disclosure

How can individuals' personal information be used and disclosed under National Privacy Principle 2.1?

An organisation may only use personal information for the primary purpose for which it is collected, and in other limited circumstances specified in NPP 2.1. The primary purpose should be narrowly and specifically defined.

Before an organisation, bound by the Privacy Act, uses personal information for a secondary purpose, such as direct marketing, it should consider whether that purpose complies with the circumstances described in NPP 2.1.

NPP 4 Security

Does the organisation need to take steps to make sure the personal information it collects is secure?

Yes, NPP 4 requires that organisations take reasonable steps to ensure that the personal information they hold is protected from misuse and loss and from unauthorised access, modification or disclosure. Scanned personal information is particularly vulnerable in this regard as the personal information is likely to be of the kind commonly used for proof of identity in other contexts, such as to establish bank accounts, obtain credit or establish identity for some government services.

As such, it is reasonable to expect that organisations that scan proof of identity documents would take particular care to ensure the security of the scanned and electronically stored personal information. These measures should include, for example, limiting staff access and using firewalls, passwords, audit trails and spyware detection. For more information about such security measures please see our website at www.privacy.gov.au/internet/tools/index.html.

NPP 4 also requires that organisations take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed. For instance, if the scanned personal information was collected to ensure the safety and security of the premises and patrons of a registered club, and no incident occurred on the date of collection, the organisation must consider whether it would need to keep the personal information after that date.

When no longer needed, the personal information should then be securely destroyed, for example, by deleting all electronic and hardcopy records of the personal information. Electronic systems often have back up processes so it would be important to make sure the personal information had been deleted from these as well.

The Office recommends that organisations set out clear guidelines as to when and how they will destroy personal information that is no longer needed.

NPP 5 Openness

What do organisations need to tell individuals about their personal information management practices?

NPP 5 requires that organisations have a privacy policy in place that describes how it manages personal information, and must make that policy available to anyone who asks for it.

In the case of scanned personal information, the policy should describe what personal information the organisation collects, how the personal information is collected and the purpose for which the organisation has collected it, as well as how the organisation stores, uses and discloses that personal information. It should also make it clear that it collects the personal information using scanning devices and, importantly, what IT security measures it has in place to protect that personal information whilst electronically stored.

Organisations may choose to provide this information to individuals at the time of collection as a means of meeting their obligations under NPP 1.3 to give the individual notice about the collection.

NPP 7 Identifiers

Can organisations scan proof of identity documents that include identification numbers issued by the Commonwealth?

Many forms of identification issued by government agencies carry what is known as an 'identifier', for example a driver's licence number. Identifiers issued by an Australian Government agency, such as a Tax File, Medicare or Passport number, must not be 'used or disclosed' by an organisation except in prescribed circumstances.

The inclusion of an identifier in a database of scanned personal information could be considered a 'use' of that personal information. As such, the organisation should consider whether it is necessary to collect that personal information in the first instance, given that the use of that identifier is likely to be prohibited by NPP 7.

What happens when scanning is done by a contractor?

In some cases, organisations may contract out the scanning of customers' identity documents, such as where licensed premises contract a security firm. If the contractor is an organisation covered by the Privacy Act, then it will have the same obligations described above.

If a contractor is not ordinarily covered by the Privacy Act, such as where it has a turnover of less than $3 million, it may come under coverage by virtue of it handling personal information for a benefit, service or advantage and so fall within the definition of 'organisation'.

Generally though, to ensure certainty, if an organisation is contracting with an organisation that is not covered by the Privacy Act it would be advisable to encourage the contractor to opt in to being covered using section 6EA of the Privacy Act. One way of doing this would be to make opting in a condition of the contract. The Office has produced an information sheet that provides further guidance on the Privacy Act and contracts. It is available at www.privacy.gov.au/publications/IS8_01.html.

Summary

Organisations should avoid routinely scanning identity documents unless the information they contain is necessary for one of its functions or activities. If there is valid reason for such scanning and collection, then the personal information must be handled in a manner that complies with the Privacy Act.

Organisations should pay particular attention to the notice they provide to individuals at the time of collecting personal information and the fact that they are required to limit the collection to that which is necessary for their functions or activities.

Organisations are also required to limit the secondary use or disclosure of the personal information, and must ensure that they have robust security measures in place to protect that personal information.

Organisations that implement practices consistent with the NPPs, including ensuring they have a privacy policy in place, are in a better position to protect their customers' privacy and to avoid having a privacy complaint lodged against them with this Office.

Further information

For further information about the NPPs, see the Privacy Commissioner's Guidelines to the National Privacy Principles and our other information sheets.

Private Sector Information Sheets

Information sheets are advisory only and are not legally binding. The National Privacy Principles in Schedule 3 of the Privacy Act do legally bind organisations.

Information sheets are based on the Office of the Privacy Commissioner's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation. Nothing in an information sheet limits the Privacy Commissioner's ability to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with. Organisations may also wish to consult the Commissioner's guidelines and other information sheets.

Office of the Privacy Commissioner

Privacy Enquiries Line **1300 363 992** - local call (calls from mobile and pay phones may incur higher charges)
TTY 1800 620 241 – no voice calls; Fax + 61 2 9284 9666; GPO Box 5218, Sydney NSW 2001.

Private Sector Information Sheet 20
Web HTML, Word and PDF published August 2007
ISBN 978-1-877079-50-4

© Commonwealth of Australia

www.privacy.gov.au