Australian Government
Office of the Australian Information Commissioner

Privacy fact sheet 5

Digital photocopiers: inadvertent collection and storage of personal information

December 2011

This fact sheet is for Australian Government agencies (s 6) and private sector organisations (s 6C) that are covered by the *Privacy Act 1988* (Cth) (Privacy Act) and that use:

- digital photocopiers, or
- multi-function printers (MFPs)

that incorporate digital scanning technology.

Some small and other businesses are exempt from the application of the Privacy Act: see privacy information sheet 12 – *2001 Coverage of and exemptions from the private sector provisions* available at www.privacy.gov.au.

Even if that is the case, it is best practice for exempt businesses to align their practices with the Privacy Act.

Most, if not all, digital photocopiers and MFPs now incorporate a digital scanner and a high-capacity hard drive which can store thousands of scanned images. Many such devices save and store scanned images created in the process of making copies, scanning documents, emailing or sending faxes.

Businesses that offer photocopying or scanning services may be inadvertently collecting large amounts of personal information from their clients.

Similarly, any agency or organisation whose employees use office facilities to scan or copy personal information may be inadvertently accumulating and storing that information.

Agencies and organisations that collect personal information, deliberately or inadvertently, may be subject to obligations under the Privacy Act in respect of the handling of that information.

'Personal information' within the meaning of the Privacy Act includes any document that contains information that can be linked with a person's identity.

This fact sheet contains suggestions and strategies for organisations and agencies to avoid the inadvertent collection of personal information through the use of photocopiers and MFPs.

Key messages

If an agency or organisation uses a digital photocopier or MFP, and those devices:

- are or may be used to scan or copy personal information, and
- store scanned images,

then the agency or organisation should ask itself:

> Is the collection and storage of personal information necessary for one of our functions or activities?

If the answer is 'no', the information should be not be retained.

The section below titled 'Avoiding inadvertent collection and storage of personal information' provides suggestions on how to prevent your photocopier or MFP from unnecessarily retaining personal information.

Obligations under the Privacy Act

The Privacy Act regulates the collection, use, storage and disclosure of personal information by agencies and organisations:

- agencies are bound by the Information Privacy Principles (IPPs) set out in s 14 of the Privacy Act

- organisations are bound by the National Privacy Principles (NPPs) set out in Schedule 3 to the Privacy Act.

In particular:

- the IPPs relevantly provide that agencies must only collect personal information for a lawful purpose directly related to their functions of activities, and where that collection is necessary for or directly related to those functions or activities, and
- the NPPs relevantly provide that organisations must only collect information that is necessary for their functions or activities.

The NPPs and IPPs are available on the OAIC website.

Where agencies and organisations collect the personal information of individuals, the Privacy Act requires them to notify the individuals of certain matters, and take measures to ensure the security of the information, including its destruction.

Agencies and organisations should set out in a document clearly expressed policies on its management of personal information, and make the document available to anyone who asks for it.

For further information on the IPPs, please see the plain English guidelines to the IPPs:

- Information Privacy Principles 1–3
- Information Privacy Principles 4–7
- Information Privacy Principles 8–11

For further information on the NPPs, please see the *Guidelines to the National Privacy Principles* available at www.privacy.gov.au.

Avoiding inadvertent storage of personal information

If you are buying or leasing a new photocopier or MFP:

- ask the manufacturer or supplier about the options available with respect to privacy and information security:
  - many manufacturers now offer models which automatically delete or overwrite scanned images once copying or scanning operations are completed
  - the ability to delete or overwrite scanned images is sometimes offered as an upgrade to base model photocopiers and MFPs.

If you already have a photocopier or MFP:

- contact the manufacturer of your photocopier or MFP, or consult your provider or technical support personnel to check whether your device stores scanned images:
  - some photocopiers and MFPs can be set to erase stored data after each operation or periodically (such as daily or weekly)
  - the manufacturer or provider for your photocopier or MFP, or your technical support staff, may be able to assist you in changing the settings on your device.
- If that cannot be done:
  - schedule regular service appointments with your device's service provider to erase scanned images stored on the integrated hard drives, or
  - consider upgrading to a device which will allow you to appropriately comply with the requirements of the Privacy Act.

Network security

If you are collecting and storing personal information, the Privacy Act requires that you take reasonable steps to make sure that information is secure and will not be accessed, modified or disclosed without authorisation (IPP 4, NPP 4).

If your photocopier or MFP is configured to store information for any amount of time (for example, the device erases stored images once a day or weekly), you may need to take steps to protect any stored personal information prior to its erasure.

Many photocopiers and MFPs are networked and may be connected to the internet. Such devices may also have the capability to send scanned images by email:

- if your device is networked, you should ensure that your network is protected behind a 'firewall', so that it cannot be accessed via the internet by unauthorised persons
- if your device is capable of sending scanned images by email, make sure that it is configured to send email to authorised accounts only (such as internal office email accounts)
- make best practice policies and processes available for your staff to follow to ensure that they maintain network security when using photocopiers and MFPs, and provide adequate training.

Selling a used photocopier or MFP/ returning a leased photocopier or MFP

It is a breach of the Privacy Act to disclose personal information outside of very specific circumstances (IPP 11, NPP 2).

As best practice, before selling or disposing of a photocopier or MFP, or returning a leased photocopier or MFP, make sure that all scanned images on the integrated hard drive have been completely erased. This may need to be done by your technical support staff, or as part of a service visit.

Make best practice policies and processes available for your staff to follow to ensure that they do not inadvertently disclose personal information when selling, returning, or disposing of a photocopier or MFP, and provide adequate training.

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information

telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 2999, Canberra ACT 2601
GPO Box 5218, Sydney NSW 2001
or visit our website at **www.oaic.gov.au**