

SEMINAR MATERIALS

Privacy Act reforms: from the IPPs to the APPs

Assessing the impact on the public sector
(federal and ACT agencies)

July 2010

PRESENTER

Jeremy Douglas-Stewart
LLB (Hons), BEc, BA

Principal Consultant
Privacy Law Consulting Australia

PRESIDIAN

LEGAL PUBLICATIONS

Disclaimer

The seminar, these seminar materials and comments by the seminar presenter are not intended to be, nor do they constitute, legal advice. Whilst the seminar and seminar materials aim to provide detailed information on privacy laws, certain issues may have been omitted and statutory provisions not addressed in order to fit within seminar delivery time-frames. Likewise, explanations provide generalised summaries of the law and, as such, do not constitute comprehensive or exhaustive statements of the law. You should seek legal and/or other professional advice, as appropriate, based on your specific circumstances before acting or relying on any of the contents of the seminar, seminar materials and/or comments of the seminar presenter.

Copyright

All legislative materials herein are reproduced by permission but do not purport to be the official or authorised versions. They are subject to Commonwealth of Australia copyright.

Copyright in this publication, excluding that relating to legislation, is owned and/or administered by Presidian Legal Publications. For reproduction or publication beyond that permitted by the *Copyright Act 1968*, permission should be sought in writing and addressed to the Copyright Officer.

© Presidian Legal Publications, Adelaide, 2010
All rights reserved

Publisher details
61 Carrington St, Adelaide
GPO Box 625 Adelaide SA 5001
DX 175 Adelaide
tel 1300 66 13 96
fax (08) 8278 9382

CONTENTS

Introduction	4
Australian Privacy Principles	7
APP 1—open and transparent management of personal information	7
APP 2—anonymity and pseudonymity	9
APP 3—collection of solicited personal information	10
APP 4—receiving unsolicited personal information	13
APP 5—notification of the collection of personal information	15
APP 6—use or disclosure of personal information	17
APP 7—direct marketing	20
APP 8—cross-border disclosure of personal information	21
APP 9—adoption, use or disclosure of government related identifiers	26
APP 10—quality of personal information	27
APP 11—security of personal information	28
APP 12—access to personal information	29
APP 13—correction of personal information	31

Australian Privacy Law Handbook

by J Douglas-Stewart (forthcoming release: September 2010)

This publication provides a detailed guide to privacy law and practice in the private and public (federal and ACT) sectors. Written in a plain-English style for privacy officers, records managers and lawyers, the text is designed to enable users to readily identify privacy obligations and to apply the laws in practice.

Practical commentary provides guidance on how privacy laws apply in the context of specific activities, ranging from core issues such as disclosing information to third parties, dealing with contractors and handling information during recruitment to peripheral issues such as disclosing health information for medical research and dealing with children.

The text includes extensive commentary and tools to assist in developing compliance measures, such as privacy policies, collection notices, consent forms, step-by-step guides and guidance on conducting privacy audits and privacy impact assessments.

The publication is updated three times per year. Each update is accompanied by an *Australian Privacy Law Bulletin* providing a report on privacy developments.

For further information, go to: www.presidian.com.au/aplh.html

To request notification of release, send a blank email to notify@presidian.com.au with "APLH" in the subject line.



PRESIDIAN
LEGAL PUBLICATIONS

Introduction

The seminar provides a detailed overview of proposed changes to the *Privacy Act 1988* (Cth) following the release of the Government's exposure draft legislation (on 24 June 2010) setting out the Australian Privacy Principles (APPs) which are to replace the public sector Information Privacy Principles (IPPs) (as well as the private sector National Privacy Principles (NPPs)).

The seminar aims to:

- provide an overview of the proposed APPs;
- undertake a gap analysis between the APPs and IPPs identifying:
 - APP obligations that are the same as, or similar to, existing IPP obligations;
 - new obligations under the APPs;
- assess the impact of the new obligations (based on the level of existing obligations);
- provide insight into how the new obligations may apply in practice;
- provide an overview of other proposed changes to the Act.

The seminar is based on an assumed familiarity with the IPPs.

Overview of Privacy Act reforms

The Government has opted to implement its reforms to the Privacy Act over two stages.

Stage one

The exposure draft legislation constitutes the first part of the Government's reforms to the Privacy Act. It has been over 20 years since the Act was originally drafted and the Government is seeking to ensure the Act remains appropriate and relevant to business practices and consumer expectations in the 21st Century. Each subsequent part of the reforms will be referred to a Senate Committee for consideration. The Government anticipates that there will be three other parts referred to the Committee as part of the "stage one" reforms. These will address:

- credit reporting – this will replace Part IIIA of the existing Act;
- the handing of health information – currently, many provisions providing for specific regulation of dealings with health information are contained in the IPPs and NPPs. These provisions do not currently appear in the APPs as the Government has not yet decided on a location for them in the new Act;
- reforms to the functions and powers of the Office of the Privacy Commissioner (with the existing office to become part of a new Office of the Australian Information Commissioner following the commencement of the *Freedom of Information (Reform) Act 2010* and the *Australian Information Commissioner Act 2010*, principally on 1 November 2010).

Once the Senate Committee has reported on all of the parts, the Government has stated that the Bill will be consolidated and introduced into Parliament.

The Senate Committee is due to report:

- on the APP exposure draft legislation by 21 September 2010; and
- on all exposure drafts of Australian privacy amendment legislation by 1 July 2011.

Stage two

The Government has indicated that its second stage of reforms will address:

- proposals to clarify or remove certain exemptions from the Privacy Act;
- the possible introduction of a statutory cause of action for serious invasion of privacy;
- serious data breach notifications;
- privacy and decision making issues for children and authorised representatives;
- handling of personal information under the *Telecommunications Act 1997*; and
- national harmonisation of privacy laws (partially considered in stage one).

The Government has not, however, set a time-frame within which these matters will be addressed.

Additional sources of regulation – regulations, rules, guidelines and privacy codes

The draft legislation envisages the following sources of additional regulation:

- Australian Privacy Rules (s 21) – these will be binding rules made by the Australian Information Commissioner. It is currently envisaged that these will apply in relation to:
 - APP 3(3)(g)(ii) regarding a collection to assist in locating a missing person; and
 - APP 6(2)(g)(ii) regarding a use or disclosure to assist in locating a missing person;
- regulations (s 22);
- non-binding Guidelines – these will be made by the Australian Information Commissioner; and
- privacy codes – under the existing Act, these enable organisations to draft their own privacy codes which, once approved, become legally binding in place of the NPPs (although there has been a very limited uptake of these codes).

Terminology – “entity”, “agency” and “organisation”

The APPs refer to “entities” to capture both agencies and organisations. Some of the APPs, however, refer specifically to organisations or agencies where there are different provisions applying to each type of entity.

Coverage of the Act

At this stage, the Government is not proposing to make any significant changes to the coverage of the Act. In particular:

- the definition of “personal information” will effectively remain the same;
- the requirement that information must be held in a record for the Act to apply (s 16B) will remain;
- key exemptions will remain, including those relating to:
 - exempt acts and practices of Commonwealth government agencies (s 7);
 - an act or practice required by foreign law (ss 6A(4) and 13D);
 - personal, family and household affairs (s 16E);
 - emergencies and disasters (Part VIA).

As noted above, the Government proposes to clarify or remove certain exemptions from the Privacy Act in “stage two” of the reforms.

In regards to extra-territorial operation, the Act currently applies to an act or practice engaged in outside of Australia where:

- it is engaged in by an organisation (but not by an agency); and
- the act or practice relates to information about an Australian citizen or permanent resident.

Under the proposed changes, the Act will apply to an act or practice engaged in outside Australia where:

- it is engaged in by an organisation *or* an agency; and
- the act relates to information about any person (ie including a foreigner) provided the entity that is dealing with the information has an Australian link (as defined by s 19(3)).

Summary of key new obligations

Key reforms made by the changes relate to:

- privacy notices, regarding the inclusion of additional information and requirements for them to be provided in a broader range of circumstances;
- privacy policies, regarding the inclusion of additional details about information handling practices;
- collection and handling of unsolicited information;
- a new category of personal information with higher levels of protection, namely sensitive information;
- restrictions on when information can be collected from a third party;
- when information can be used and disclosed for secondary purposes;
- overseas disclosures, regarding steps that must be taken to ensure the information will continue to be under appropriate levels of protection and potential liability of agencies for breaches by overseas recipients;
- destruction or de-identification of information once it is no longer needed;
- notification of third parties to whom information has been previously disclosed of corrections that are made to the information;
- rights to deal with agencies anonymously or under a pseudonym;
- express obligations to develop and implement compliance programs.

Tables of APPs and IPPs

APPs
APP 1 – open and transparent management of personal information
APP 2 – anonymity and pseudonymity
APP 3 – collection of solicited personal information
APP 4 – receiving unsolicited personal information
APP 5 – notification of the collection of personal information
APP 6 – use or disclosure of personal information
APP 7 – direct marketing
APP 8 – cross-border disclosure of personal information
APP 9 – adoption, use or disclosure of government related identifiers
APP 10 – quality of personal information
APP 11 – security of personal information
APP 12 – access to personal information
APP 13 – correction of personal information

IPPs
IPP 1 – manner and purpose of collection of personal information
IPP 2 – solicitation of personal information from individual concerned
IPP 3 – solicitation of personal information generally
IPP 4 – storage and security of personal information
IPP 5 – information relating to records kept by record-keeper
IPP 6 – access to records containing personal information
IPP 7 – alteration of records containing personal information
IPP 8 – record-keeper to check accuracy etc. of personal information before use
IPP 9 – personal information to be used only for relevant purposes
IPP 10 – limits on use of personal information
IPP 11 – limits on disclosure of personal information

Australian Privacy Principles

APP 1—open and transparent management of personal information

- (1) The object of this principle is to ensure that entities manage personal information in an open and transparent way.
Compliance with the Australian Privacy Principles etc.
- (2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that:
 - (a) will ensure that the entity complies with the Australian Privacy Principles; and
 - (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles.

Purpose (APP 1(2))

The Government's *Companion Guide – Australian Privacy Principles* (June 2010) outlines the purpose of APP 1 as follows (at 9):

The requirement for open and transparent management is the first of the Australian Privacy Principles because it will emphasise that entities should first plan *how* they will handle personal information before they collect and process it.

The principle is also intended to outline that part of complying with the Australian Privacy Principles is making sure that entities consider their privacy obligations when planning new systems.

This is part of international moves towards a “privacy by design” approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception. (emphasis in original)

Accordingly, APP 1(2) aims to ensure that entities take a *proactive* approach to privacy compliance (ie foreseeing privacy risks and putting systems in place to avoid such risks eventuating), rather than a *reactive* one (eg resolving privacy issues and complaints as they arise, resulting in privacy policies and procedures being developed piecemeal).

Equivalent IPPs

Obligations under APP 1(2) have no express equivalent under the IPPs (although such obligations are, to a large extent, implicit).

Impact of changes (APP 1(2))

Level of impact: medium

(i) Measures to ensure compliance (APP 1(2)(a))

Whilst the IPPs do not expressly require an agency to take reasonable steps to implement practices, procedures and systems to ensure compliance, it has nevertheless been a practical reality for many agencies that such measures need to be taken as part of risk management programs to comply with the Act. For such agencies, APP 1(2) will have little impact as it is merely formalising a practical requirement that already exists under the IPPs.

However, APP 1(2) does have ramifications for agencies that have *not* adopted practices, procedures and systems to ensure compliance where it would be *reasonable* for them to do so. Entities that may fall within this category could, for example, include a small agency which has not formalised its information handling procedures by developing relevant policies and internal guidelines, which deals with sensitive issues and which considers privacy matters are partially or largely covered by other laws or governance mechanisms impacting on information handling practices (eg duties of confidence and records management laws).

Such an agency will need to:

- consider whether it is reasonable for it to adopt practices, procedures and systems to ensure compliance (in view of factors such as the sensitivity of information held and cost); and
- if so – develop and maintain them.

(ii) “Deal with inquiries” about compliance (APP 1(2)(b))

The obligation to have in place practices, procedures and systems to enable an agency to deal with enquiries regarding compliance with the APPs has the potential to be significant, including for large agencies with well established privacy compliance programs. Similar obligations exist under IPP 5 (“Information relating to records kept by record-keeper”) which require agencies to be open and transparent regarding what types of personal information they hold and how it is handled. However, APP 1(2)(b) has a different focus; namely, on enquiries regarding compliance, as opposed to types of information held and how such information is handled.

In effect, APP 1(2)(b) will require agencies to have in place practices and procedures that require staff to respond in an appropriate way to privacy enquiries. Depending on the circumstances, it may be “reasonable” to “deal with inquiries” by providing individuals with a copy of the agency’s privacy policy (assuming it is sufficiently detailed and accurate to address the issues raised). In other instances, it may require more onerous steps, such as requiring the relevant staff member to refer the enquiry to a manager or Privacy Contact Officer who can provide an informed and considered explanation in response to the specific issues raised.

A type of scenario that APP 1(2)(b) is likely trying to avoid is where an individual raises a privacy concern, for example, with a client services officer when completing an application form (eg “Why are you asking for this information?” or “Who will this information be disclosed to?”) and the client services officer in effect provides a response that avoids or deflects the question (eg “Don’t worry. Information is treated confidentially and we won’t disclose it to anyone”, even though this is not correct, or “There is nothing to be concerned about – we are bound by the Privacy Act.”). Policies and procedures that result in responses such as these would not appear to meet APP 1(2)(b) requirements to have systems in place to enable the agency “to deal with inquiries or complaints”.

Privacy policy

- (3) An entity must have a clearly expressed and up-to-date policy (the **privacy policy**) about the management of personal information by the entity.
- (4) Without limiting subsection (3), the privacy policy must contain the following information:
 - (a) the kinds of personal information that the entity collects and holds;
 - (b) how the entity collects and holds personal information;
 - (c) the purposes for which the entity collects, holds, uses and discloses personal information;
 - (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
 - (e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;
 - (f) whether the entity is likely to disclose personal information to overseas recipients;
 - (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

Equivalent IPPs (APP 1(3) and (4))

APP 1(3) reflects obligations under IPP 5.3 to maintain what has become known as Personal Information Digests. However, APP 1(3) refers to the document as a “privacy policy” and specifies different types of information that must be contained in the document. Obligations under IPP 5.3 and 5.4 regarding requirements to prepare, maintain and make available Personal Information Digests have, in effect, been replaced by the obligation to maintain a privacy policy.

“Overseas recipients” (APP 1(4)(f))

A disclosure to an overseas recipient will, in addition to including a transfer of information to a person overseas, also encompass circumstances where information that is stored in Australia (eg on a network) is accessed by someone overseas.

Impact of changes (APP 1(3) and (4))

Level of impact: medium

Many agencies already have privacy policies. Such agencies will need to redraft their policies to meet the requirements of APP 1(3). Agencies that do not have a privacy policy will need to develop one.

The types of information referred to in APP 1(4)(a)-(e) are commonly included in privacy policies and can be easily inserted into existing privacy policies if not already included.

The types of information referred to in APP 1(4)(f) and (g) regarding overseas disclosures and the countries in which recipients are located are rarely included in privacy policies. Accordingly, agencies will need to review what types of information they disclose to overseas recipients and incorporate the relevant details into their privacy policies. Whilst the inclusion of such information might be of concern to private sector organisations (wishing to protect the confidentiality of, for example, their outsourcing practices and location of foreign service providers), it is of less concern to agencies owing to the fact that such practices are less common in the public sector and, where they do occur, there is often no commercial confidentiality surrounding the practices.

Agencies will no longer be required to prepare annual Personal Information Digests by virtue of the fact that this obligation has been substituted by the obligation to have a privacy policy.

Availability of privacy policy etc.

- (5) An entity must take such steps as are reasonable in the circumstances to make its privacy policy available:
 - (a) free of charge; and
 - (b) in such form as is appropriate.
- (6) If an individual requests a copy of an entity's privacy policy in a particular form, the entity must take such steps as are reasonable in the circumstances to give the individual a copy in that form.

Form of privacy policy (APP 1(6))

Ideally, guidance from the Privacy Commissioner will clarify whether it will be sufficient in all cases for agencies to make privacy policies available in electronic and, if appropriate, hardcopy formats. If not, agencies may also need to make privacy policies available in alternative formats where it is reasonable to do so – for example, by providing a verbal explanation for a blind person.

APP 2—anonymity and pseudonymity

- (1) Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.
- (2) Subsection (1) does not apply if:
 - (a) an entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves; or
 - (b) it is impracticable for an entity to deal with individuals who have not identified themselves.

Equivalent IPPs

APP 2 has no equivalent under the IPPs.

Impact of changes (APP 2)

Level of impact: medium

Agencies will need to consider the circumstances in which it is lawful and practicable to deal with clients anonymously. Such circumstances will generally be relatively limited, but will nevertheless exist in some instances – for example, in relation to individuals:

- making general enquiries over the phone or online;

- accessing free counselling services;
- who wish to remain anonymous for cultural reasons.

If such circumstances exist, agencies will need to implement systems that enable individuals to deal with them anonymously or under a pseudonym. The fact that existing systems and administrative arrangements do not currently enable an agency to deal anonymously is unlikely to mean that it will not be “practicable” to deal anonymously.

APP 3—collection of solicited personal information

Personal information other than sensitive information

- (1) An entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.

Equivalent IPPs (APP 3(1))

The obligations under APP 3(1) reflect obligations under IPP 1.1 to only collect information for “a lawful purpose directly related to a function or activity” and where the information “is necessary for or directly related to that purpose”. The wording of APP 3(1) is, however, more clear and concise.

Impact of changes (APP 3(1))

Level of impact: low

In view of the close similarities between APP 3(1) and IPP 1.1, APP 3(1) will have minimal impact in regards to collections of solicited information.

Sensitive information

- (2) An entity must not collect sensitive information about an individual unless:
- both of the following apply:
 - the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities;
 - the individual consents to the collection of the information; or
 - subsection (3) applies in relation to the information.
- (3) This subsection applies in relation to sensitive information about an individual (the ***affected individual***) if:
- the collection of the information is required or authorised by or under an Australian law, or an order of a court or tribunal; or
 - both of the following apply:
 - the entity reasonably believes that the collection of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
 - it is unreasonable or impracticable to obtain the affected individual’s consent to the collection; or
 - both of the following apply:
 - the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;
 - the entity reasonably believes that the collection of the information is necessary in order for the entity to take appropriate action in relation to the matter; or
 - both of the following apply:
 - the entity is an enforcement body;
 - the entity reasonably believes that the collection of the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or

- (e) both of the following apply:
 - (i) the entity is an agency;
 - (ii) the entity reasonably believes that the collection of the information is necessary for the entity's diplomatic or consular functions or activities; or
- (f) the entity is the Defence Force and the entity reasonably believes that the collection of the information is necessary for any of the following occurring outside Australia:
 - (i) war or warlike operations;
 - (ii) peacekeeping or peace enforcement;
 - (iii) civil aid, humanitarian assistance, medical or civil emergency or disaster relief; or
- (g) both of the following apply:
 - (i) the entity reasonably believes that the collection of the information is reasonably necessary to assist any entity, body or person to locate a person who has been reported as missing;
 - (ii) the collection complies with the Australian Privacy Rules made under paragraph 21(a); or
- (h) both of the following apply:
 - (i) the information is collected by a non-profit organisation and relates to the activities of the non-profit organisation;
 - (ii) the information relates solely to the members of the non-profit organisation, or to individuals who have regular contact with the organisation in connection with its activities; or
- (i) the collection of the information is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or
- (j) the collection of the information is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Overview of (APP 3(2) and (3))

APP 3(2) and (3) generally provide that “sensitive information” (as defined) can only be collected where:

- it meets the “functions test” and the individual has consented; or
- an exception under APP 3(3) is applicable (none of which require satisfaction of the functions test or consent).

Equivalent IPP obligations

APP 3(2) and (3) have no equivalent under the IPPs which (unlike the NPPs) do not distinguish between “personal information” and “sensitive information” (as defined by the Act). Accordingly, the collection of sensitive information by agencies under the IPPs is not subject to any restrictions that do not apply to personal information generally.

Additional obligations

The fact that APP 3(2) and (3) regulate the collection of sensitive information separately from other types of personal information and have no equivalent under the IPPs means that obligations under APP 3(2) and (3) constitute an entirely new framework for the collection of what is in effect a new category of personal information for agencies.

“Sensitive information”

APP 3(2) and (3) apply in relation to “sensitive information” as defined by the Act.

Sensitive information will be defined to mean (s 15):

- information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record;

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

Impact of changes (APP 3(2) and (3))

Level of impact: high

Many agencies collect relatively large amounts of sensitive information (particularly relative to private sector organisations). For example, an agency might collect:

- information about racial origin and religious beliefs (eg when handling complaints about discrimination);
- health information (eg about clients and employees);
- criminal records (eg when conducting background checks); and
- biometric information (eg for use in relation to biometric access controls).

As such, APP 3(2) and (3) have the potential to have a major impact on agencies' collection practices. Agencies will need to review what types of sensitive information they collect and ensure the collections of such information are permitted under APP 3(2) and (3).

Agencies will in particular need to look closely at collections of sensitive information that occur without consent (eg when conducting investigations) to ensure they are permitted under one of the exceptions under APP 3(3). An exception that is likely to be heavily relied upon in this regard is APP 3(3)(a) which permits collections of sensitive information without consent if the collection is required or authorised by or under law. This exception will, for example, likely permit collections made when conducting investigations pursuant to statutory functions or powers that directly envisage such collections taking place.

Means of collection

- (4) An entity must collect personal information only by lawful and fair means.
- (5) An entity must collect personal information about an individual only from the individual unless:
 - (a) if the entity is an agency—the entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to collect the information other than from the individual; or
 - (b) it is unreasonable or impracticable to do so.

Equivalent IPP obligations (APP 3(4) and (5))

APP 3(4) reflects IPP 1.2 which prohibits collections by unlawful or unfair means.

APP 3(5) has no equivalent under the IPPs – currently, agencies are under no obligation to collect information directly from an individual where, for example, it is reasonable and practicable to do so.

Impact of changes (APP 3(4) and (5))

Level of impact: high

APP 3(4) will have minimal impact on information handling practices in view of similar obligations under IPP 1.2.

However, APP 3(5) will have a significant impact as it introduces a new set of obligations on agencies in regards to collections from third parties. In effect, APP 3(5) prohibits a collection from a third party unless one of the exceptions under APP 3(5)(a) or (b) apply.

Agencies commonly collect personal information about individuals from a large number of third parties – for example, other agencies, family members, medical practitioners and businesses. Agencies will need to review all such collections and assess whether they meet the requirements of either

APP 3(5)(a) or (b). If not, the agency will need to cease those types of collections and develop policies, procedures and systems to ensure that such information is only collected directly from the individuals concerned.

Solicited personal information

(6) This principle applies to the collection of personal information that is solicited by an entity.

“Solicited”

Proposed s 15 defines “solicits” as follows:

an entity solicits personal information if the entity requests a person to provide the personal information, or to provide a kind of information in which that personal information is included.

As such, information will likely be solicited if an agency asks for:

- specific information – such as on a form requesting name and DOB; or
- broad categories of information – such as:
 - an application form requesting reasons as to why an individual believes a decision that has been made is unfair; or
 - an online form seeking feedback about services provided.

Solicited information will not, for example, include information contained in a letter from a member of the public providing a confidential tip-off about suspected fraud where the agency has not requested such information and has no statutory responsibilities or functions to investigate such frauds.

Scope of APP 3 – solicited collections only

APP 3(6) limits the application of APP 3 to solicited collections of personal information (although, in the absence of the word “only” before “applies”, it could be interpreted as being intended to clarify that APP 3 applies to solicited collections *in addition to* unsolicited collections). Accordingly, APP 3 does not apply in relation to collections of unsolicited personal information (including unsolicited sensitive information) – such collections are regulated under APP 4.

APP 4—receiving unsolicited personal information

- (1) If:
 - (a) an entity receives personal information about an individual; and
 - (b) the entity did not solicit the information;
 the entity must, within a reasonable period of receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.
- (2) The entity may use or disclose the personal information for the purposes of making the determination under subsection (1).
- (3) If the entity determines that the entity could have collected the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had so collected the information.
- (4) If the entity determines that the entity could not have collected the personal information, the entity must, as soon as practicable but only if it is lawful and reasonable to do so:
 - (a) destroy the information; or
 - (b) ensure that the information is no longer personal information.

Equivalent IPPs

The IPPs do not have equivalent provisions to APP 4.

IPP 2 (regarding privacy notices at the time of collection) and IPP 3 (requiring that information be relevant to the collection purpose, up-to-date, complete and not collected in an unreasonably intrusive way) apply only to *solicited* collections – they do not apply to *unsolicited* collections.

IPP 1 (which requires information to be necessary for a function or activity and collected fairly and lawfully) makes no distinction between solicited and unsolicited collections and, as such, is generally understood to apply to both. In the context of the private sector NPPs, it is well established that a collection of unsolicited personal information is a collection of personal information for the purposes of the Act (see, eg, *M v Financial Institution* [2009] PrivCmrA 16 and *E v Private School* [2010] PrivCmrA 6). There is nothing to suggest the position is any different under IPP 1. Accordingly, an agency is, for example, required to ensure that a collection of unsolicited information is necessary for a function or activity under IPP 1.1. In this regard, IPP 1 is similar to APP 4(1) (ie an agency is required to assess whether the unsolicited collection is permitted against the general criteria for collections under IPP 1.1).

Operation (APP 4)

APP 4 requires an agency that receives unsolicited personal information to consider whether it would have been permitted to collect the information under APP 3 if it had solicited the information.

In particular, it must ensure that:

- if the information is not sensitive information – the information is reasonably necessary for, or directly related to, one or more of the agency’s functions or activities (APP 3(1)); or
- if the information is sensitive information (APP 3(2)) –
 - both of the following apply:
 - the information is reasonably necessary for, or directly related to, one or more of the agency’s functions or activities; and
 - the individual consents to the collection of the information; or
 - one of the exceptions under APP 3(3) applies to the information.

If the collection would not be permitted under APP 3, the agency must generally destroy or de-identify the information, unless it is unlawful or unreasonable to do so.

Interaction with *Archives Act 1983*

The obligation for agencies to destroy information is a significant one in view of obligations under s 24 of the *Archives Act 1983* not to destroy a Commonwealth record (within the meaning of that Act) unless, among other things, required to do so by law. If an agency is considering destroying all information in a record and, hence, destroying the record itself, the agency must ensure this is permitted under the Archives Act (see, for example, the Australian Government Management Advisory Committee’s *Note for File: A Report on Recordkeeping in the Australian Public Service* (2007) which provides guidance on when Commonwealth records, including low-value documents, can be destroyed).

Impact of changes (APP 4)

Level of impact: high

Agencies will be under significant new obligations in regards to collections of unsolicited information by virtue of the fact that obligations under APP 4 that are equivalent to those under IPPs 2 and 3 (which only apply to solicited collections) apply to both solicited *and* unsolicited collections.

For example:

- An agency currently has no notification obligations under IPP 2 in regards to collections of unsolicited personal information. An agency will now have notification obligations under APP 5 in regards to such collections.
- Agencies are often in receipt of unsolicited sensitive information about third parties (eg a letter reporting suspected fraud by a person providing details about the person's criminal record). In regards to such collections, agencies will now need to assess whether the information could have been collected pursuant to APP 3(2)(b) (in reliance on one of the exceptions under APP 3(3)) if it were solicited (it will not be permitted under APP 3(2)(a) as the individual concerned will not have consented to the collection).

APP 4(4) imposes significant limitations in regards to handling unsolicited information. For example, the requirement to destroy or de-identify such information under the principle appears to effectively prevent an agency from opting to forward information to another appropriate agency where, for example, the relevant unsolicited information was sent to it in an erroneous belief that it was the relevant authority to handle a particular matter.

Agencies will need to undertake comprehensive audits to identify what types of unsolicited information they collect and develop systems to ensure they are handled in accordance with APP 4.

APP 5—notification of the collection of personal information

- (1) At or before the time or, if that is not practicable, as soon as practicable after, an entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:
 - (a) to notify the individual of such matters referred to in subsection (2) as is reasonable in the circumstances; or
 - (b) to otherwise ensure that the individual is aware of any such matters.
- (2) The matters for the purposes of subsection (1) are as follows:
 - (a) the identity and contact details of the entity;
 - (b) if:
 - (i) the entity collects the personal information from someone other than the individual; or
 - (ii) the individual may not be aware that the entity has collected the personal information;
 the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
 - (c) if the collection of the personal information is required or authorised by or under an Australian law or an order of a court or tribunal—the fact that the collection is so required or authorised (including the name of the Australian law, or which order of a court or tribunal requires or authorises the collection);
 - (d) the purposes for which the entity collects the personal information;
 - (e) the main consequences (if any) for the individual if all or part of the personal information is not collected by the entity;
 - (f) any other entity, body or person, or the types of any other entities, bodies or persons, to which the entity usually discloses personal information of the kind collected by the entity;