

Privacy; a right worth protecting...

Peggy Cheong,
President,
Law Society Northern Territory



As people and communities become more developed and sophisticated, it appears that there are more and more rights of a personal nature crystallising which require definition and protection on a legal basis. People now expect a right to maintain their privacy, and expect their private information to be preserved and not shared with anyone who is not authorised or allowed to have access to that information. Perhaps this has always been an expectation of the people which had not previously been articulated, but is something which is being advocated for strenuously now and into the future.

There have been National Privacy Principles (NPPs) in place in Australia for a number of years. These however, are set to be refined and overtaken by revised principles known as the Australian Privacy Principles (APPs). From 12 March 2014, the APPs will replace the NPPs and will apply to organisations and Australian Government (including Norfolk Island Government) agencies.

The Commonwealth reforms set out in the new APPs will impact on the Northern Territory, principally on Territory businesses and NGOs with an annual turnover of \$3m, and on Commonwealth Departments work in the Territory. In addition, there are other categories in the Territory that will also have to comply with the Federal legislation and this includes private schools, private sector health service providers and

credit providers. Usually Northern Territory government authorities are generally only required to comply with the NT *Information Act*, although there are a few exceptions.

Briefly, (and I mean very briefly), there are 13 APPs:

APP 1

APP 1 deals with open and transparent management of personal information and the object of this principle is to ensure that APP entities that are required to comply with the Federal legislation, manage personal information in an open and transparent way. APP 1 requires an APP entity to take such steps as are reasonable in the circumstances to implement practices, develop policies, procedures and systems relating to the entity's functions and activities to ensure that it complies with the APP and which will allow the entity to deal with inquiries or complaints from individuals about its compliance with the APP.

APP 2

APP 2 deals with anonymity and pseudonymity, and provides that individuals must have the option of not identifying themselves or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. The exception to this requirement is if the APP entity is required or authorised by

or under an Australian law or Court order to deal with individuals who have to identify themselves, or, if it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

APP 3

APP 3 deals with the collection of personal information and sets out the process, procedure and system of the collection of such information. This APP relates to collection of solicited personal information, and different means of collection may apply to sensitive information as compared to non-sensitive information.

APP 4

APP 4 refers to with how an APP entity is to deal with unsolicited personal information. It sets out a process and procedure whereby the APP entity has to decide how and what to do with unsolicited personal information that it has received and whether or not the entity can disclose the said personal information. If the APP entity determines that it would not normally have been collected the personal information through the APP, and the information is not contained in a Commonwealth record, then the entity must as soon as practicable and only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

APP 5

APP 5 deals with the notification of the collection of personal information. It provides that at or before the time or, if that is not practicable, as soon as practicable after, if an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters referred to in APP 5.2, or to otherwise ensure that the individual is aware of any such matters.

APP 6

APP 6 deals with the use or disclosure of personal information. Overall APP 6 provides that if an APP entity holds personal information about a person that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless the person has consented to the use or disclosure of the information, or, if subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information. APP 6.2 relates to situations where the person would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is **directly** related to the primary purpose (with respect to sensitive information), or if the information is related to the primary purpose (with respect to not sensitive information). APP 6.3 relates to APP entities which are not an enforcement body and the information is biometric information or templates, and the recipient of the information is an enforcement body and the disclosure is conducted in accordance with guidelines made by the Commissioner for this purpose.

APP 7

APP 7 deals with direct marketing, namely if an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing. There are exceptions to this requirement in circumstances where the organisation collected the information from the individual and the individual would reasonably expect the organisation to use or disclose the information for that purpose, and the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation, and the individual has not made such a request to the organisation. Other exceptions in relation to the application of APP 7 include consent from the individual and the organisation is a contracted service provider for the Commonwealth.

APP 8

APP 8 deals with cross border disclosure of personal information. The general rule from APP 8 is that before an APP entity discloses personal information about an individual to a person (the overseas recipient), who is not in Australia or an external territory, and who is not the entity or the individual, the entity must take such steps as are reasonable to ensure that the overseas recipient does not breach the APP (other than APP 1) in relation to the information. Once again there are exceptions to this rule in APP 8.2.

APP 9

APP 9 deals with the adoption, use, or disclosure of government related identifiers (GRD's). This provides that an organisation must not adopt a GRD of an individual

as its own identifier of the individual unless the adoption of the GRD is required or authorised by or under an Australian law or court order; or if the GRD is prescribed by the regulations and the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations, and the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

APP 10

APP 10 refers to the quality of personal information, and provides that an APP entity must take such steps as are reasonable to ensure that the personal information that the entity collects is accurate, up to date and complete. The APP entity must also take steps as are reasonable to ensure that the personal information that the entity uses or discloses, is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

APP 11

APP 11 deals with the security of personal information, and provides that if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances, to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure. If the entity no longer needs the information that it holds, and the information is not contained in a Commonwealth record, and the entity is not required by law or court order to retain the information, the entity must take such steps as are reasonable to destroy the information or ensure that the information is de-identified.

APP 12

APP 12 deals with access to

personal information and provides that if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. Once again, not surprisingly, there are exceptions to access, for example, if the APP entity is an agency and is required or authorised to refuse to give the individual access to the personal information under the *Freedom of Information Act* or any other Act of the Commonwealth, of a Norfolk Island enactment that provides for access by persons to documents. Further exceptions to access also include situations where the entity reasonably believes that giving access would:

- pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or, have an unreasonable impact on the privacy of another individual; or
- the request for access is frivolous or vexatious; or
- the information relates to existing or anticipated legal proceedings between the entity and the individual and would not be accessible by the process of discovery in legal proceedings; or
- would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- giving access would be

unlawful; or

- denying access is required or authorised by or under an Australian law or Court order; or
- the entity has reason to suspect unlawful activity, misconduct of a serious nature that relates to the entity's functions and providing access would prejudice the taking of appropriate action in relation to the matter; or
- giving access would prejudice one or more enforcement related activities conducted by or on behalf of an enforcement body; or, lastly,
- giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

APP 12 also deals with how an APP entity is to deal with requests for access and other means for access for individuals if access is refused by the entity.

APP 13

Lucky, APP 13 refers to correction of personal information and provides that if an entity holds personal information about an individual, and the entity is satisfied that the information is inaccurate, out of date, irrelevant or misleading; or the individual requests the entity

to correct the information, the entity must take such steps as are reasonable to correct that information to ensure that it is up to date, accurate, complete, relevant and not misleading. If an APP entity corrects personal information about an individual that the entity had previously disclosed to another APP entity, and the individual requests the entity to notify the other APP entity of the correction, then the entity must give such notification unless it is impracticable or unlawful to do so. APP 13 also deals with situations where the entity refuses to correct the personal information and the issue of a statement arising from such refusal. It also sets out how an entity is to deal with requests for correction and the timeframe for same.

With the revised and renewed APPs on privacy of personal information, no organisation or entity should fall short of being better able to request, obtain, hold, share, disclose (or not) personal information; and when all is said and done, the same organisation and entity should also be able to correct, destroy or de-identify the information that it has held. In this age of computer wizardry, is any information, personal or otherwise truly ever lost, deleted or destroyed on web-land and cyberspace?... as I'm quite sure that some (if not all) of my personal information is floating on a cloud somewhere over the Darwin.... ●



Head to the Law Society Website, www.lawsocietynt.asn.au, and click on the links.