What to check when subscribing to online services – a privacy perspective.

Does the service provider have a clearly expressed and up to date privacy policy available on their website?

The service provider should have a clearly expressed and up-to-date privacy policy that sets out the personal information they collect and what they do with it. The privacy policy should clearly set out the following information (see the items below) in an open and transparent manner.

Does the service provider give you the option of anonymity or pseudonymity?

Check whether the site allows you to enter a pseudonym, or to remain anonymous by not requiring you to enter your name or other identifying information.
If this is the case, avoid entering your personal information to reduce the risk to you in the event of a data breach of the site or service.

What personal information is being requested from me, and is all of the information requested necessary for the provision of services?

When subscribing to services, some personal information may need to be given to service providers, in order for them to provide those services to you, and to limit access. However, in some instances service providers will ask for more information than is really necessary. If they ask for personal information of a sensitive nature, or personally identifiable information, such as your Date of Birth or license number for example, you should consider whether it is necessary for the provision of services and therefore whether to provide that information or not.

Does the service provider adequately explain the purpose for seeking the personal information?

If a service provider can provide reasoning for the collection of your personal information you are in a better position to make a judgement on whether to provide that information based on your personal situation and your own assessment of any risk in providing that information.

The purpose the service provider outlines for the collection of personal information should explain why they need the specific personal information they are requesting of you and how it relates to the provision of services to you.

Does the online service provider outline what processes it follows if they receive unsolicited personal information?

If a service provider receives personal information about an individual, that they did not request, they should explain the actions they would take to ensure the protection of that additional personal information.

Does the online service provider take reasonable steps to notify the individual of certain matters or ensure that the individual is aware of those matters?

The online service provider should notify the individual or ensure the individual is aware of the following matters:

- the online service providers identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law

- the purposes of collection
- the consequences if personal information is not collected
- the service providers usual disclosures of personal information of the kind collected by the service provider
- information about the service provider's privacy policy
- whether the service provider is likely to disclose the personal information to overseas recipients and if practicable the countries in which they are located.

The service provider must take reasonable steps before, or at the time it collects the personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

Does the service provider outline the purpose for which the information is being collected, or disclosed?

The service provider should be open and transparent about the use and disclosure of personal information and clearly outline the purpose(s) for which it will be used or disclosed.

If the purpose for which the information is being collected or disclosed is not relevant to the provision of the service(s) this would need further consideration by the individual prior to providing personal information to this service provider.

Does the service provider intend using your personal information for direct marketing?

The service provider may wish to use or disclose your personal information for the purposes of direct marketing. If this is the case, the individual should be provided with the option to be excluded from these direct marketing activities. If there is no option to be excluded from this direct marketing, the individual should make the assessment whether this is acceptable prior to subscribing to the service.

Does the service provider transfer your personal information to other companies or utilise overseas locations for data storage or processing?

Online service providers could be located virtually anywhere in the world. Australia's Privacy Act is enforceable only on Australian organisations and so it is important to know whether data is being sent overseas, and to which countries, so that you can assess the specific country's record with respect to ensuring privacy. It will then be a decision you make on whether you are comfortable with your data being sent overseas, and subscribe to the service.

Even if the online service provider is located in Australia, it is very common for online services to utilise other online service providers – some of which may be overseas – and therefore they may transfer some of your personal information overseas.

Does the service adopt, use or disclose government related identifiers?

There are restrictions on the adoption, use and disclosure of government related identifiers (e.g. Medicare Number, Tax File number etc.) and if requested, or used within the service, this would need to meet certain requirements as set out in the Privacy Act. If this is not clearly explained in the privacy policy, this could be reason for some concern and serious consideration given prior to providing this information.

Does the service provider explain the reasonable steps it will take to ensure the accuracy and currency of the personal information collected?

If your personal information changes, how does the service provider ensure that the information they hold is updated and accurate? This should be clearly explained in their privacy policy.

Does the security provider explain what reasonable steps it will undertake to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure?

The service provider should outline the security measures it will have to ensure the protection of your personal information either in their Privacy Policy, or elsewhere on their site – possibly a Security page. This information should be checked to ensure that the individual is comfortable with the steps that are being taken to protect the information, prior to subscribing to the service.

Does the service provider outline how they will respond to individual requests for access to personal information held?

The service provider should outline how they will handle any requests for access to personal information, including how to contact them for such requests.

How long does the service provider retain your personal information?

It is important to understand what the service provider will do with your personal information if you were to unsubscribe from the service. The service provider should provide details of how long they will retain your information once you unsubscribe and when they will delete it.

Use of apps and services

Other considerations when subscribing to, or utilising, mobile apps and services.

Geolocation metadata in photos/images

Most cameras and smartphones store geolocation metadata with the digital image/photo. If the app or service you are using includes functionality to upload digital photos or images, consideration should be given to whether you wish to have this geolocation metadata available to others who may access the photo/image. Malicious actors could access this metadata to identify where the photo was taken.

To avoid storing the geolocation metadata with the digital photo/image, check the device manual to disable this feature.

Sharing of photos/images

Prior to sharing any photos or images online or through an app, ensure consideration is given to whether the photo or image is appropriate for sharing through that platform.

Location Services on mobile apps

Many mobile apps utilise location services. The apps will therefore use the GPS to collect information about where you are located. This can certainly be useful in apps, such as Google Maps to help identify where you are in a given setting and guide your travel. However, due consideration should be given prior to enabling this for other apps that may not have as clear a reasoning for this to be enabled. If it is not clear as to why the mobile app would need access to your location, do not enable location services for that mobile app.