KEEPING YOUR ONLINE PERSONAL INFORMATION PRIVATE – CAN IT BE DONE?

The Urban Myth

Facebook is the social media of choice and it is estimated that approximately 12 million Australians use Facebook on a daily basis.

It should not come as a surprise that privacy hoaxes (and its variations) have been circulating on Facebook for years. The hoax claims that Facebook users who wish to retain control over their photos and contents should post a 'privacy notice' on their profile.

For example:

> *"I do not give Facebook or any entities associated with Facebook permission to use my pictures, information, or posts, both past and future. By this statement, I give notice to Facebook it is strictly forbidden to disclose, copy, distribute, or take any other action against me based on this profile and/or its contents. The content of this profile is private and confidential information."*

Every so often, the hoax re-appears on your Facebook wall. After all, it hardly takes any time and effort for someone to copy, paste and post the 'privacy notice'. However, does such 'privacy notice' really work and more importantly, have you lost control of your privacy to Facebook?!

Reality

There is no need to panic. Everything that you post on Facebook e.g. photos, posts, even the 'privacy notice', belongs to you. This is confirmed in Facebook's Terms of Service (which explicitly states that "*you own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings*" (https://www.facebook.com/legal/terms/update).

Level 2, 111 Wellington Street, East Perth WA 6004 • PO Box 6314, East Perth WA 6892
T: +61 8 9388 3100 • F: +61 8 9388 3105 • E: reception@murfett.com.au
ABN 74 120 362 825 • W: www.murfett.com.au

Before a user can use Facebook, the user must first accept Facebook's legal terms which includes its Terms of Service and Privacy Policy. The user's acceptance of Facebook's legal terms cannot be amended by simply posting a 'privacy notice', like the above example post. If a user does not agree with Facebook's policies, the user can either:

- not use Facebook i.e. decline to set up an account;
- cancel their Facebook account (if they already have one, taking note that this is different from simply deactivating the account); or
- negotiate modified legal terms with Facebook (good luck with that!).

In short, you own your content and you can control how such content is shared i.e. who can see your content, by utilising your privacy settings.

How can I be certain that any personal information I provide to a government agency is safe?

Recently, there was public outcry over the 2016 census as privacy advocates called on the Australian Bureau of Statistics (**ABS**) not to collect the names and addresses of Australians.

In previous censuses, names and addresses were destroyed approximately eighteen months after the census. However, the ABS announced that for the 2016 census they would extend this retention period to four years. It also emerged that the ABS was cross-referencing names and addresses against records held by other government agencies. This led to some people declaring that they would boycott the census on privacy grounds.

The handling of individual's personal information is governed by the *Privacy Act* 1988 (Cth), which was substantially updated again in 2016 (**Privacy Act**).

The Privacy Act and its Australian Privacy Principles

The Privacy Act regulates the collection, use, storage and disclosure of personal information by agencies or organisations. It also permits the handling of health information for health and medical research purposes in certain circumstances where researchers are unable to seek an individual's consent.

As an Australian Government agency, the ABS is required to comply with the Privacy Act and handle personal information in accordance with the mandatory Australian Privacy Principles (**APPs**).

The APPs outline how Australian and Norfolk Island Government agencies and all private sector or not-for-profit organisations with an annual turnover of more than $3 million must handle, use and manage personal information. An explanation of the APPs can be found at the Officer of the Australian Information Commissioner's website (https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles).

Level 2, 111 Wellington Street, East Perth WA 6004 • PO Box 6314, East Perth WA 6892
T: +61 8 9388 3100 • F: +61 8 9388 3105 • E: reception@murfett.com.au
ABN 74 120 362 825 • W: www.murfett.com.au

You may also have responsibilities under the Privacy Act if your business falls within one of the following categories:

- private sector health service providers, including child care centres, private schools and private tertiary educational institutions;
- businesses that sell or purchase personal information;
- credit reporting bodies;
- contracted service providers for a Commonwealth contract;
- employee associations registered or recognised under the *Fair Work (Registered Organisations) Act 2009*;
- businesses that have opted-in to the Privacy Act; or
- businesses prescribed by the Regulations as part of the Privacy Act.

If your business collects personal information from customers/clients and staff (e.g. through, customer contact details & credit application forms, your business' employee/HR records etc) or even just from 'visitors' (e.g. through your website) it is essential that you familiarise yourself with your internal privacy policies, processes and procedures.

You should have a readily available privacy policy available on your website and in your business that customers/clients and staff can read before they provide you with their personal information.

There are very significant civil penalties & fines for contravening the Privacy Act.

A severe breach will not only impact the organisation financially, it is very likely that the organisation's reputation will suffer a detrimental impact as well (as seen in the case of Ashley Madison).

Privacy Amendment (Notifiable Data Breaches) Act 2017

Further, pursuant to the new *Privacy Amendment (Notifiable Data Breaches) Act 2017*, it established a Notifiable Data Breaches (**NDB**) scheme in Australia. The NDB scheme requires organisations covered by the Privacy Act:

- to notify any individuals likely to be at risk of serious harm by a data breach; and
- to report such to Office of the Australian Information Commissioner (https://www.oaic.gov.au), so that the risks associated with the breach can be evaluated.

A NDB is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

Level 2, 111 Wellington Street, East Perth WA 6004 • PO Box 6314, East Perth WA 6892
T: +61 8 9388 3100 • F: +61 8 9388 3105 • E: reception@murfett.com.au
ABN 74 120 362 825 • W: www.murfett.com.au

The NDB Scheme will commence on 22 February 2018 and only applies to eligible data breaches that occur on, or after, that date.

Government organisations and businesses will benefit greatly from proactively having appropriate privacy policies and controls in place.

For further information contact Murfett Legal by telephone on +61 8 9388 3100, via our website at www.murfett.com.au or email one of the following directors:

Jason De Silva : jason.desilva@murfett.com.au

Kelly Parker : kelly.parker@murfett.com.au

Peter Broun : peter.broun@murfett.com.au