Minimum Standards for Personal Information

The minimum standards for any organisations handling large volumes of Australian personally identifiable information (PII) online should be **significant**. Further, such organisations should be required to report on their security posture to a government agency annually.

These non-trivial imposts should be offset by the ability for many organisations to be able conduct their business without any retaining any PII at all.

The easiest way to avoid data breaches containing email addresses and password hashes is to never store that information at all.

Most businesses do not actually require PII. They simply require –

- a method to authenticate you
- a name to call you
- a method of contacting you
- a method of accept payment from you
- a method to deliver to you
- an identifier suitable for law enforcement purposes

For example, Sign in with Apple allows you to pseudonymously sign up to apps and websites through their 'Hide My Email' feature. Apple provides those apps and websites with –

- a highly secure passwordless method of authenticating you
- a pairwise pseudonymous email address to contact you
- a pseudonymous method of accepting payment, and
- an identifier that is suitable for law enforcement to determine your identity if required.

This should be the norm for small, medium and many large businesses.

Australian identity providers, such as the government and financial institutions, should be encouraged to provide pairwise pseudonymous authentication services. (The Australian Government's current Digital Identity framework does not yet support this. Further, the ability to establish an identity completely online, while commercially attractive, is actually likely to exacerbate cyber identity theft scenarios.)

Australia Post and other delivery providers should provide pairwise pseudonymous delivery addresses. Australia Post Parcel Locker numbers are a step towards how this might work.

Google, Microsoft and other email/messaging providers should be encouraged to provide services similar to Apple's.

Online payment providers should be encouraged to provide pairwise pseudonymous payment identifiers.

Australian telephony providers should plan for an ecosystem that allows pairwise pseudonymous telephony identifiers.

John Uhlmann
Cyber Security Researcher