

Public and yet still “private”

This is a pre-release edited version of a column appearing in Online Banking Review, June 2010.

Privacy is a notoriously slippery topic, but information privacy law in fact is pretty straightforward. Having said that, the implications of privacy law are counter-intuitive, and this has led to some infamous missteps. In this edition, I’m going to review privacy law, and look at how some of the big Internet brands continue to misunderstand privacy technicalities, at their peril. It’s early days but already there are crucial lessons on how publicly available data from social networks can be used by financial institutions.

There can be endless arguments about the meaning of privacy. Not only is it intensely personal, it also ranges across philosophy, human rights, civil liberties and politics. Yet Australia’s Privacy Act, like most such legislation worldwide, neatly side steps the moral and philosophical minefields.

Paradoxically, words like “private” and “public” aren’t used in the Privacy Act. Instead what matters is *personal information*, namely any information or opinion about an individual where their identity is “apparent or can reasonably be ascertained”. Note that privacy law only applies to businesses and governments.

Consultants often advise that privacy and security are different things. And so they are, but more even importantly, privacy has little to do with confidentiality or secrecy either. The National Privacy Principles—enshrined in the private sector extensions made in 2000 to the Privacy Act—are all about *control*.

- The **Collection Principle** means a business generally cannot gather (or even create) personal information if it is not required for a defined business function, and without the individual’s consent.
- The **Use & Disclosure Principles** mean that information gathered (or created) for one purpose cannot be used for unrelated secondary purposes without consent, nor disclosed to unrelated parties.
- And the **Access & Correction Principles** mean that an individual usually has the right to be given access to all personal information held by a business about them, and to have any errors fixed.

Some of the implications may be surprising. For one, privacy law is blind to how information is collected. It doesn’t matter how personal information comes to be in your business; even if personal information is generated internally from audit logs or evaluative processes, once

you have it, you are deemed to have made a *collection* according to privacy law. Moreover, if personal information is collected from the public domain, it may still be subject to privacy law.

An important current case is that of Google and its collection of wifi data from open networks by its Street View cars. Some argue it’s careless for people to not encrypt their wireless setups, but the fact is that data gathered by sniffing networks is subject to the Privacy Act if it relates to individuals that can be identified (and with Google’s vast linked databases, working out identities is assumed to be within their powers). A person has not agreed to the exploitation of their information merely because they might be lax with their security.

So what does information privacy law mean for banking and social networking?

First and foremost, even if information is “public”, it is still subject to the Privacy Act. If a bank takes part in social networking, and for example creates groups through which it tries to research customer preferences, it should do so overtly. People making revelations online are not necessarily giving implied consent for their personal information to be put to use for secondary commercial purposes. So banks making use of this technology must make full and clear disclosures about why they collect information, and what they intend to do with it.

Of course the greatest value created by social networking is the metadata generated by the network as it evolves. There is real treasure to be found in the myriad interconnections, and what they can reveal about relationships, communities, markets and trends. One advantage of taking a bird’s eye view is that we can afford to de-identify the raw data and move out of the remit of the Privacy Act.

Some say privacy law hasn’t kept up with technology. For the most part, conventional privacy law is actually quite clear about the rights of individuals to control who knows what about them. But networking technology does challenge privacy principles. For if building networks leads to discoveries that aren’t apparent until critical mass is reached, then it’s just not possible to inform members up front about the precise purpose of collection. Instead, businesses should share the spoils of social networking with their customers, who typically gladly opt in if properly rewarded for participating in what is still a great big experiment.