Get off my cloud: when privacy laws meet cloud computing

Jake Goldenfein

What does privacy mean in an age of ongoing privacy breaches? With new privacy law coming online in Australia on March 12, our Privacy in Practice series explores the practical challenges facing Australian business and consumers in a world rethinking privacy.

The growth of cloud computing has revolutionised the way that information is produced, stored, processed and consumed, with privacy laws sometimes failing to keep up.

From March 12, 2014, changes to Australia’s Privacy Act will impose new obligations on companies that collect and process personal information, including those that operate in the cloud.

Cloud computing involves using technical infrastructure, controlled by another party, to store information or data.

As well as data storage, some cloud services include features that trade on the personal information they generate. For example, online services like Facebook, Gmail, and other Google offerings remain “free”, but users must provide personal information to obtain access. The data transmitted through these entities may be subject to increased movement between organisations, increasing exposure to processes like data matching and mining.

Data is the ‘new oil’

The “new oil” of these economies is data created by the provision of personal information online. As personal devices become “thinner”, an increasing amount of information processing occurs external to that device on servers operated by commercial enterprises in various places.

Think of e-readers, which offer connections to the vast repertories of books located in expansive data warehouses, accessed by an authorised account, and governed by licensing agreements. While users access content, the content-providers are collecting the personal information generated by users. Further, the terms of access to those services are often vague or unclear, and may provide undesired revenue streams to data controllers through tracking and profiling or even offering other entities access to your information.

This trend towards increased storage and processing of personal information in external data centres controlled by companies that trade in personal information raises significant questions about surveillance and control.
The “thinner” the device, the more transparent the individual becomes, as more data is provided to third parties. This emphasises the importance of effective privacy regimes. Surveillance problems are compounded if information is transmitted through overseas jurisdictions that are not subject to Australian privacy legislation, meaning users have no recourse to Australian enforcement mechanisms (which are relatively limited anyway).

The main threats to privacy in this context therefore include:

- personal information being collected, used or stored not in accordance with a user’s wishes;
- inappropriate or unauthorised access to personal information in the cloud through security vulnerabilities or weak access control;
- uncontrolled copies of data being duplicated within the cloud;
- users agreeing to be tracked or profiled in ways that they were not aware of;
- exposure of personal information to third parties without consent; and
- function creep (the use of data for a purpose different to that for which it was given).

Data protection to the fore

For those reasons, data protection regimes such as the Australian Privacy Act, are becoming more important – both for entities attempting to establish cloud services in Australia, and Australians whose information is being stored and processed offshore.

The Privacy Act was introduced in response to the perceived threat from increased computing capacity and the undue influence that institutional databases may have over the lives of their data subjects.

The Privacy Principles articulated in the Act reflect a belief that individuals “should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations”. But new communications technologies have the capacity to undermine those goals, suggesting privacy regimes need updating.

To manage the risks associated with cloud services, changes to the Privacy Act will require users and operators of cloud services to adhere to new standards.

Organisations that use data storage located outside Australia must disclose (in their privacy policy) which country is hosting those servers, and the individual whose information has been collected must be notified.

Further, before an organisation that has collected personal information can disclose it to a cloud provider overseas, it must take reasonable steps to ensure that the recipient will not breach the Privacy Principles. This can occur through contractual arrangements, or
may be satisfied if the cloud storage company is subject to privacy laws which are similar to the Australian privacy laws, including the availability of enforcement mechanisms.

“Deeming” provisions may render the Australian information sender liable for the overseas recipient’s treatment of personal information. There are also obligations to take “reasonable steps” to protect information from misuse, interference, loss, unauthorised access, modification and disclosure, which may impose additional obligations if the data is stored overseas.

While these amendments may offer greater protection to the providers of personal information, they have been criticised as lacking clarity for cloud services-providers due to the technology-neutral nature of the changes.

For instance, other jurisdictions distinguish between the obligations of a “data controller” – an entity that actively controls personal information and the purposes for which it is used – and a “data processor” – who only processes personal information according to the wishes of the data controller (a distinction implicated in the difference between Infrastructure as a Service and Software as a Service cloud configurations). This means data processors may be subject to obligations that more appropriately apply to controllers, such as the provision of access and correction of data.

Contrary to older ideas of the internet as a decentralised or distributed medium, cloud computing has created colossal data centres which concentrate vast amounts of personal information in amalgamated nodes.

More work is needed to assess whether the changes to Australia’s privacy laws will effectively regulate the risks posed by the centralisation of personal information offshore.