Privacy and Cross Border Transfer of Information

The Inquiry would value views on the costs, benefits and trade-offs of the following policy options or other alternatives:

- *Review and assess the new privacy requirements two years after implementation to consider whether the impacts appropriately balance financial system efficiency and privacy protections.*
- *Review record-keeping and privacy requirements that impact on cross-border information flows and explore options for improving cross-border mutual regulatory recognition in these areas.*

This submission should be read after the submission by Kevin Cox titled "Government Support for an User Centric Electronic Identity System"

Particular Australian Privacy Principles applicable to this submission are:

Australian Privacy Principle 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

1. *the individual has consented to the use or disclosure of the information; or*
2. *subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.*

and

Australian Privacy Principle 8 — cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

1. *who is not in Australia or an external Territory; and*
2. *who is not the entity or the individual;*

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Most people would consider the visits they make to websites to be private and do not want others recording their visits. Widespread tracking of website visits and the selling of that information is a multi-billion dollar business. This tracking breaks both APP6 and APP8. There are a variety of methods used, the simplest of which is third party cookies. A third party cookie is an identifier put on a person's browser by a website. Other websites can read the third party cookie and then ask the website who put the cookie on the website information obtained about the person.

Any Australian Website who puts third party cookies onto a person's browser and releases information to other parties without the informed consent of the person, is likely to be violating both principles even if there appears to be no direct information about a person supplied by the Australian Website.

If a person has visited a website then that fact, if passed on, is now available to participating websites who subscribe to the service. This information can be collated so that pieces of information such as the person's name, email address, date of birth, sex, buying habits, travel plans etc. are available to all participating websites. This is clearly a violation of both principles because these services are international.

The Australian Government could stop tracking from Australian websites by fining Australian organisations who put any form of tracking mechanism on their websites and allowing that information to be obtained by any other organisation.

Tracking can serve a useful purpose for users. However its indiscriminate use is privacy unfriendly and it is economically inefficient. It has the same characteristics as spam email and the more it used the less value for each impression because the advertised switch off. This is evidenced by the drop in cost per impression. It is also evidenced by the increasing support for "Do Not Track" legislation from many in the advertising industry.

If however, the advertising industry only sent ads to people who were receptive to the message then the Cost per Impression would increase. Rather than using the techniques of "Big Data" to try to guess what people want, the advertising industry could ask people what messages they wanted to receive. This could be achieved if the person themselves was the only one who had access to information about their online behaviour and was able to tailor the delivery of advertising messages. This would immediately increase the Cost per Impression and would be economically efficient.

This approach would also benefit law enforcement. When law enforcement needed to find out about a person's online activities they could obtain a warrant to examine the person's own individual record of online behaviour. They would not need to conduct bulk surveillance of the regular channels of communications.

Recommendation

The government make it known that it will enforce Australian Privacy Principle 6 and 8 and fine websites that send information about website visits to a third party. This should coincide with government support for giving individuals access to their own personal information held by government.