INTERNET SAFETY INSTITUTE

The adequacy of protections for the privacy of Australians online

Submission of the Internet Safety Institute
to the Senate Standing Committee on Environment, Communications and the Arts

Alastair MacGibbon
23 July 2010

Background

On 24 June 2010 the Senate referred the following matter to the Senate Standing Committee on Environment, Communications and the Arts for inquiry and report:

The adequacy of protections for the privacy of Australians online, with regard to

(a) privacy protections and data collection on social networking sites;
(b) data collection activities of private companies;
(c) data collection activities of government agencies; and
(d) other related issues.

About the Internet Safety Institute

The Internet Safety Institute was founded in December 2008 to provide an honest and informed view of issues facing online consumers, businesses and governments. Through thought leadership, public comment, research and education, we aim to advance the cause of safety on the internet. The founders of the Internet Safety Institute are experienced in the field of online consumer protection.

The author of this submission, Alastair MacGibbon, most recently spent 4 and a half years as head of Trust, Safety and Customer Support for eBay Australia and later eBay Asia Pacific. Prior to eBay, MacGibbon was the founding Director of the Australian High Tech Crime Centre, and was a Federal Agent with the Australian Federal Police for 15 years. As a consequence of his government and commercial experience, MacGibbon has worked in the field of internet crime from a national policing and a corporate perspective, has dealt with consumer victimisation and corporate survival in the online space, has championed consumer education and driven a range of public private partnerships aimed at reducing internet crime.

The situation

The Australian public has a huge appetite for mobile and internet technologies, with amongst the world's highest adoption rates for social networking, mobile and "smart" phones (such as Blackberries and iPhones) and internet connectivity as a whole. Increasingly internet services are accessed via mobile phones, and information is stored in "the cloud", both of which will bring about the next wave of societal issues.

The use of various internet and mobile technologies has changed the amount of personal information Australians are *giving away*, having *collected* and *stolen* from them.

Summary of recommendations

- Companies operating on the internet should state their use of data collected as a consequence of using their services and to do so in plain language.

- Online consumers should expect - and governments compel - companies to institutionalise privacy, including the adoption of routine privacy impact assessments conducted by privacy professionals.

- Businesses providing services to Australians should be held accountable if they fail to protect (or if they misuse) personal data. In an internet increasingly dominated by companies providing services via "the cloud", it is essential that such responsibility extend to data pertaining to Australians which is held offshore, and for companies domiciled offshore providing services to Australians, to be brought under the same requirements.

- A robust data loss notification regime should be implemented, coupled with sanctions available to the Office of Privacy Commissioner (which also needs to be appropriately funded and resourced).

- A right to civil action by those wronged will help market forces bring in robust IT security, encryption, data handling and privacy policies.

- The Australian government should work to harmonise data access regimes that are agnostic in terms of how and where data is stored.

- Australian agencies should have an ability to compel access to data, even if held offshore by a foreign-domiciled company.

- The Australian Government should commence negotiations for an international data access and privacy regime: an agreed level playing field that encourages the efficient and free flow of data while bringing stability and predictability to domestic governments.

Giving away information

The social networking phenomenon has induced a step-change in the amount of previously "personal" information voluntarily uploaded for public consumption: creating an indelible chronological (and increasingly mapped) record of our behaviour, thoughts and associations. "Our" record is added by us, as well as by friends and associates outside our control, the technologies deployed (such as photo recognition/tagging and geolocation), and the ability to search for and link people to each other and to events.

While we do need to teach people about the consequences of their actions online, especially young people, in time the ubiquitous nature of that information will mean we change how we judge people: unlike the past where many of our actions and words faded; in our connected world we will all have done things we regret (or which are taken out of context) that are now available to those who want to know and thereby present new risks, but many of those risks will be offset by what we can refer to as a sort of "mutually assured humiliation."

A more pernicious privacy threat: data collection

While we knowingly upload certain private information, our interactions with technology generates other information about us that is collected on a scale that almost beggars belief. Private corporations now hold more data about individuals than even the most authoritarian governments could dream.

In Western countries we are used to media, regulatory, legislative and judicial oversight of the actions of governments and the data held and used by governments. The pace of technological change has meant that such oversight has not been applied to corporate control of personal information.

In spite of this, the public seems to trust public institutions less than many companies whose sole existence is to deliver "shareholder value". At least some of that trust is misplaced.

On the internet very little is really free: "free" services are provided so companies can build their brand, increase adoption of their services, collect data (contact details, interests, behaviour), sell advertising, and carry out a range of other money making activities.

Some companies have been able to build revenue streams of billions of dollars by providing free services to consumers that dominate much of the internet, from search, to advertising, to mapping, to web analytics.

Online companies can now make enormous profits by "monetising" personal data through what is known as behavioural marketing.

The concept of geolocation, increasingly possible by the use of mobile handsets to access internet services allowing triangulation and/or GPS coordinates to be captured, will see a further step change in personalised advertising, including the possibility of broadcasting the consumer's location to advertisers.

Much online data is collected in a manner unknown to the users of technology, even though - most times - they have accepted a “user agreement” or some similar disclaimer at the time of engaging the service. The simple reality is that people do not read the fine print.

Companies operating on the internet should state their use of data collected as a consequence of using their services and to do so in plain language.

Online consumers should expect - and governments compel - companies to institutionalise privacy, including the adoption of routine privacy impact assessments conducted by privacy professionals.

Death by a thousand cuts: poor security degrades privacy

Privacy cannot be protected if there is a poor security culture on the part of the end user or the companies who have access to and store their personal data.

Criminals are adept at stealing financial credentials and other personal data from legitimate businesses. Other criminals target home computers using malicious software (malware) to steal sensitive data or trick consumers via phishing or fraudulent websites.

Criminals have been stunningly successful in stripping our most sensitive information. And then parading it on online black market portals. So far the best protection we have had against victimisation is criminal inefficiency. Not their ability to get hold of the data - rather their lack of capacity to exploit it. It is a very important distinction.

Businesses providing services to Australians should be held accountable if they fail to protect (or if they misuse) personal data. In an internet increasingly dominated by companies providing services via “the cloud”, it is essential that such responsibility extend to data pertaining to Australians which is held offshore, and for companies domiciled offshore providing services to Australians, to be brought under the same requirements.

As such, a robust data loss notification regime should be implemented, coupled with sanctions available to the Office of Privacy Commissioner (which also needs to be appropriately funded and resourced).

In addition, a right to civil action by those wronged will help market forces bring in robust IT security, encryption, data handling and privacy policies.

We should not be scared of legislative regimes that enshrine privacy in both the public and private sectors: predictability and stability brought through sensible regulation will create a more trusted and trustworthy internet, which will in turn stimulate growth.

Government access to data

The cloud also brings the dilemma of government access to private data. Clearly there will be instances when it is proper for government agencies to gain access to private data, as long as threshold criteria are met. There are inconsistencies currently where thresholds for access to data online are too low compared with offline, and other times where government is unable to obtain data it should.

For example:

Scenario 1 - a suspect's email data at rest in a laptop in a house would require police to obtain a search warrant to enter the building and seize the laptop.

Scenario 2 - a suspect uses an Australian email provider offering web based access and storage (cloud) which would only require the police to serve the ISP with a form signed by a senior police officer.

Scenario 3 - a suspect uses a foreign web based email service. The email provider may totally disregard a police request for data, assuming the police knew how to contact the provider in the first place.

The Australian government should work to harmonise data access regimes that are agnostic in terms of how and where data is stored.

Australian agencies should have an ability to compel access to data, even if held offshore by a foreign-domiciled company.

In the long term the Australian Government should commence negotiations for an international data access and privacy regime: an agreed level playing field that encourages the efficient and free flow of data while bringing stability and predictability to domestic governments. Something akin to an international law of the sea.

Conclusion

We would happily provide further information to the committee should it require it.

Alastair MacGibbon
23 July 2010