The adequacy of protections for the privacy of Australians online

Submission to the Senate Standing Committee on Environment, Communications and the Arts

John Scott

30 September, 2010

Background

On the 24 June 2010 the Senate referred the following matter to the Environment, Communications and the Arts References Committee for inquiry and report by 20 October 2010:
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 Author

John Scott is the Vice President of the Australian Risk Policy Institute, Co-Chair of the Renal Services Advisory Meeting for the Canberra Hospital, and Director of ScottCromwell Pty Ltd. He was previously a member of the Senior Executive Service with the Commonwealth Department of Community Services and Health providing specialized expertise in very large scale networking of the health sector for the purposes of improving communications; communications at times of highly sensitive personal information.

The Situation

The nature of organisations and services

The nature of the organisations and the services we obtain from them can be increasingly characterized as:

a) Organisations are not defined by buildings and employees, rather they increasingly consist of loose networks of services;

b) These services are increasingly provided by a dynamically changing group of employees, contractors and sub-contractors;

c) The nature of these services also change over time—sometimes at relatively short notice; and,

d) These services operate on a network of machines; some within the organisation and some scattered around the country and indeed on occasion around the world; many of the machines are wireless and increasingly not owned by the organisation.

The contribution of the Internet and Web

The OECD and US National Science Foundation in their 'Workshop on the Future of the Internet'[1] held in Paris on 8 March, 2006 made the following points:

[1] WORKSHOP "THE FUTURE OF THE INTERNET": PROCEEDINGS, *co-organised by the Organisation for Economic Co-operation and Development, and the US National Science Foundation held in Paris on 8 March 2006.*

a) Strong economic and social drivers for the Internet mean that the world's societies and economies increasingly depend upon the Internet.

b) Opportunities offered by faster, more capable, and increasingly pervasive IP (Internet protocol)-based applications at the service level, both wired and wireless, are accompanied by issues that need addressing at the infrastructure level, including ensuring reliability and manageability, security and privacy, interoperability of the network of networks, and enabling the global open exchange of information and views.

c) Most challenges are not solely technical but are rooted in issues of economics, ownership and trust. In particular, no one "owns" the security issues.

d) There is a need for sustainable business models to support the deployment of infrastructure.

In the period following the issuing of the Workshop Proceedings the focus has begun to shift from the wide-open Web to semi-closed environments (called platforms) and 'applications' that operate in these environments. In these situations the Internet is used simply for transport. This reflects the fact that the Web is an application on top of the Internet, where the Internet provides the transport.

Two prominent examples of these semi-closed environments are the Apple iPhone with its downloadable applications (apps) and Facebook.

This architecture of semi-closed platforms with applications existing on top of the Internet represents a revolution. It does not mean that the Web will disappear; it does mean that more and more of the investment will be channelled into these environments; environments which are semi- to fully-closed, and often, proprietary networks. These environments offer significantly better prospects than the web to obtain a return on investment. It is this new environment to which we must address our concerns and find our solution frameworks for the identification and management of risk; of which the risk to privacy is a key concern.

The Consumer Experience

Consumers are increasingly choosing these new 'platforms' because often they just work better or fit into people's live. We favour convenience and reliability.

As a consequence the amount of personal information Australians are providing, having collected and equally stolen from them is increasing.

The public's use and comfort with this new environment will depend significantly upon whether they are convinced that the privacy and security of their personal data can be guaranteed.

Equally, from a civil society perspective, the rapid development and expansion of the Internet and more recently these new environments is not without its own threats. The demand for rights to privacy and security of personal data equally has to be matched with personal and organisational responsibilities to act in a manner which helps to maintain and enhance civil society.

A higher level trust among the collaborating partners is required to operate in this emerging environment; a much higher level than is present today.

The Risk Policy Model

Society is very demanding regarding accountability for the things that go wrong when there are suitable means for dealing with uncertainty and risk. The Australian Risk Policy Institute, in August 2010, released a new approach to Risk Management designed to assist in the identification and

management of risks, including privacy risk, in a world of networks; a world of increasing uncertainty and disorder.

Key features of the Risk Policy Model include:

a) Recognising and using 'Networks' – global and local - external and internal – as the key new source of risk identification

b) Recognising the existence of 'Systemic' risks – which may cover whole systems in society, government or business, may be ongoing, may be outside direct control thus potentially unmanageable, and may not exist in one location or place

c) Recognising 'Vulnerability' as a critical, new risk identification criterion – vulnerability is very different from risk and needs to be added to risk management frameworks

d) Relating 'Time' to vulnerability as another critical, new risk identification criterion – it is necessary to understand that risks may occur at different times in processes or events and may be missed if time is not considered as part of vulnerability in risk identification.

The Risk Policy Model offers a way to look at risk at the whole-of-system level. This is the level at which society will increasingly have to address privacy and other risks.

Summary of Recommendations

- Recognise that the online world is changing; changing quite dramatically with both opportunities and risks.
- Recognise that the shift from the Web to new application environments is where people will increasingly commit time because these platforms make it possible to behave in a different way; a way that works better and fits into their lives.
- Recognise that the governance of these platforms offers opportunities to establish principles and norms guiding and governing the behaviour of the people who use the services as well as the organisation and the service providers themselves.
- Appreciate that what is required to properly address privacy is the elevation of risk from management to policy; policy being the highest level of purpose.
- Use the Risk Policy Model as the basis for approach privacy in a world of networks.

Conclusion

I would be happy to discuss this further.

John Scott

30 September 2010