Senator Senator Catryna Bilyk
Chair Joint Select Committee on Cyber Safety
PO Box 6021
CANBERRA ACT 2600

Enquiries: Siobhan Jenner
Tel: (02) 80191603
Our ref: A11/0271
Your ref:

Attn: Jane Hearn
Secretary of the Committee
jscc@aph.gov.au

29 July 2011

Dear Senator Bilyk

Re: Inquiry into Cybercrime Legislation Amendment Bill 2011

The Office of the Privacy Commissioner NSW is pleased to be able to make a submission to the Joint Select Committee on Cyber Safety regarding the Inquiry into Cybercrime Legislation Amendment Bill 2011(the Bill), however the short period of time provided by the Committee in which to respond means that this submission is necessarily limited to high level matters and to a small number of suggested amendments.

Under section 36(2) of the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) the Privacy Commissioner has the power, among other things, to make public statements about matters relating to the privacy of individuals generally and to make recommendations about any matter that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals.

Preservation regime

It is my understanding that the Bill will allow cognate amendments to the *Telecommunications Act 1997* (Cth) (T Act), the *Telecommunications (Interception and Access) Act 1979* (Cth) (T(IA) Act), the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (MACM Act) and the *Criminal Code Act 1995* (Cth) and these amendments will enable the Australian Government to sign up to the *Council of Europe Convention on Cybercrime* (the Convention). While these laws are all Commonwealth Acts, they potentially affect the privacy expectations of all residents of NSW. As Acting Privacy Commissioner I generally support measures to combat the potential appropriation of the identity of individuals for criminal or other purposes as long as those measures are proportionate to the

seriousness of the conduct at issue and other matters such as the likelihood of the conduct occurring.

From the Bill and Explanatory Memorandum it appears that Schedule 1 of the Bill will amend the T Act and the T (IA) Act to require carriers to 'preserve' certain stored communications, (which in my view would be likely to include personal information of the sender or receiver), upon the giving of a notice by Australian law enforcement bodies for historic or on-going domestic purposes or in the case certain foreign countries by the Australian Federal Police.

Mutual assistance application

As I understand it Schedule 2 of the Bill will amend the MACM Act, the T Act and the T (IA) Act to enable foreign countries which are signatories to the Convention make a request directly to Australian law enforcement bodies for access to data held by carriers or carriage service providers, instead of them having to submit a formal request for assistance to the Attorney General. Law enforcement bodies will be able to disclose the requested information directly to the requesting foreign law enforcement body.

Under the amendments in Part 2 of the Bill, a foreign law enforcement body will be able to obtain prospective telecommunications data provided that it makes a 'mutual assistance application' and if the application has been authorised by the Attorney General.

Privacy considerations

As I understand it, the 'preservation' scheme may only take effect where there is reasonable suspicion of 'serious infringements' of Australian and/or foreign laws. Of concern to me are the provisions which will amend the MACM Act to enable the Attorney General to authorise the 'Australian Federal Police or a police force or a police service of a State' to apply for a warrant under the T(IA) Act seeking access to communications stored by a carrier if:

> (a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the *requesting country*) has commenced in the requesting country; and
>
> (b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:
>
> > (i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
> >
> > (ii) a fine of an amount that is at least equivalent to 900 penalty units; and

(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and

(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications[1].

The required preservation of certain computer communications by carriers and the disclosure of that information to foreign countries represents a significant privacy intrusion into the private activities of Australian telecommunication users, but one which I recognise must be balanced against the significant harm, or potential harm caused to individuals and/or nation states by serious criminal activities such as child pornography, identity fraud and theft, computer hacking or other serious cyber crime. The open-ended nature of the matters in subsection (b) means that these offences may not be prohibited under Australian law. For instance I note that the Convention requires that member states enact laws for the prosecution of matters such as the infringement of copyright and related rights[2]. As I understand it, copyright infringement is a civil not a criminal matter in Australia.

In my view, personal information about Australian citizens should not be made available to foreign countries for the purpose of prosecuting individuals for conduct which would not constitute an offence in Australia. As I understand it the legal principle *ignorantia juris non excusat* is generally held to only apply to laws within a particular jurisduction not to the world at large especially where the indivual is not resident in that foreign jurisdiction at the time of the alleged offence. Support for my broad position is sourced in the fact that the current proporals require an amendment and formal depature from existing laws which enshrine existing rights and third party obligations. This is howver coupled with the emerging and to date new discrete issues that apply to cyber related scope and functionality.

In addition, while I note that the Bill requires some consideration of the impact on the privacy of individuals affected by a 'mutual assistance application'[3] or by the issuing of an authorisation[4] to use or disclose information or documents, there is no guidance as to the weight to be given to those considerations and the circumstances, if any, in which the negative impact upon the expectation of privacy will outweigh the matters in the application.

Finally, I am pleased to note that the Bill contains offence provisions for improper use and disclosure of information or documents obtained under the scheme[5]. Given the fact that much of the information is likely to

[1] Subsection 15B MACM Act
[2] Article 10, the Convention.
[3] Subsection 15B MACM Act
[4] Subsection 180F T(IA) Act
[5] Schedule 4 T(IA) Act

constitute personal information or in the case of documents contain personal information this will go some way to protecting the privacy of individuals who will be affected by the scheme. However in light of the recent investigations by the Office of the Australian Information Commissioner[6] in relation to data breaches, I suggest that the Bill goes further in this regard by imposing an obligation not only to take reasonable steps to secure the information and documents but to notify subject individuals at the time of the data breach.

In light of my concerns about the Bill I suggest that there be further opportunity to comment not only on the Bill, but also on the privacy impact of the Mutual Assistance scheme generally. If this is not possible I suggest that the Bill be subject to a Privacy Impact Assessment which will make patent the privacy risks and hopefully improve the privacy protections in the Bill.

Yours sincerely

John McAteer
Acting Privacy Commissioner
Information and Privacy Commission

[6] See http://www.oaic.gov.au/news/statements/statement_investigation_into_Sony_data_breach.html and http://www.oaic.gov.au/news/media_release_vodafone_omi.html