Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

5 August 2011

Senator Catryna Bilyk
Chair, Joint Select Committee on Cyber-Safety
Parliament of Australia

Dear Senator Bilyk

Re: Cybercrime Legislation Amendment Bill 2011

Thank you for the opportunity to appear before the Committee on Monday 1 August to give oral evidence. We took several questions on notice and I attach our answers, together with one additional submission.

We repeat our call for your committee to send this Bill back to the Department, and require any future re-submission to be accompanied by more complete and adequate information and more reasoned justification for a more limited set of amendments.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation (02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

Supplementary Submission to the Joint Select Committee on Cyber-Safety

Inquiry into Cybercrime Legislation Amendment Bill 2011

Answers to questions taken on notice at Committee hearing on 1 August 2011

Q1. Further detail of our concerns about the lack of 'dual criminality' criteria (section 5.5 of our initial submission.

Answer:
We respectfully suggest that these concerns are more than adequately explained in several of the other submissions – including those from the Law Council of Australia, the Queensland and New South Wales Councils for Civil Liberties, and the Cyberspace Law and Policy Centre.

Q2. Further information about other jurisdictions in which there is a greater degree of transparency about the use of powers to intercept or access communications data.

Answer:
Our US colleagues confirm our reference to notification of wiretaps as follows:

> "both of the US laws that allow for government interception of communications - The federal wiretap act and FISA - require notice to every person who is subject to a government wiretap though there are provisions for delayed notification that are frequently invoked."

A UK colleague advises:

> "There is nothing in UK law that would specifically require law enforcement agencies to pro-actively inform data subjects that their communications have been accessed even once such knowledge would no longer prejudice investigations. If a law enforcement agency obtains personal data about an individual by accessing their communications data then the normal provisions of the Data Protection Act [and Freedom of Information Act] still apply and, potentially, they should be given fair processing information. However it is difficult to see any circumstances where communications data would be accessed without one of the exemptions [to access in both the DPA and the FOIA] coming into play. Whist … it would nevertheless be good practice to provide this information once the risk of prejudice is passed … would be hard pushed to maintain that the DPA actually requires it."

There is detailed guidance on this issue in two Codes of Practice issued by the UK Home Office in relation to the Regulation of Investigatory Powers Act (RIPA) – which is the UK equivalent of the TIAA – see http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/ We note the following statement in the Code on Acquistion and Disclosure of Communications Data:

> 7.4 There is no provision in the Act preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA

We cannot immediately point to any other jurisdictions where there is greater transparency but have asked our international colleagues and will forward any further relevant information we receive.

Q3. Our views about the time periods specified in the Bill

Answer:
As we said in oral evidence, in response to questions, any time limits are to some extent arbitrary, but we would have expected a better attempt at explaining and justifying the periods in the Bill in the Explanatory Memorandum. A flow chart or diagram would be helpful to show the various scenarios under which information might be firstly preserved, and then accessed either by warrant (for stored communications) or by an authorization (other data).

We note that the 90 days is the 'maximum' period specified in the Convention, and that provision of a renewal option is left to the discretion of Parties. The government should explain why it has chosen both the maximum period, and the option of renewal for an unlimited number of successive periods.

The provision for renewal means that the issue is not so much whether 90 days is long enough for effective investigation as it is whether 90 days is an appropriate interval for review and re-issue of a notice.

Ongoing domestic preservation notices apply to information received by the Carrier/CSP within a period of 29 days after receipt of the notice, whereas historic preservation notices (both historic domestic and all foreign notices) apply to information held at any time between receipt of the notice and the end of that day (i.e. a maximum of 24 hours). Again, we submit that the Committee should question the justification for the 29 days, which appears not just arbitrary but also odd.

We note that foreign preservation notices have no default expiry date because their use is tied to mutual assistance processes. The issuing agency (always the AFP) has to revoke a foreign preservation notice within 3 days of the Attorney General refusing a mutual assistance request or an overseas agency withdrawing the request. But we note that a foreign preservation notice stays in effect for up to 180 days even if no mutual assistance request is made. We further note that the Explanatory Memorandum justifies the need for Schedule 2 Part 2 on the basis that:

> "Article 30 of the Convention requires Australia to facilitate the **expeditious** partial disclosure of traffic data to foreign countries.... (page 16, our emphasis).

In light of this the 180 days seems excessive and we submit that a much shorter default period should apply.

We certainly support the submissions that have called for clear destruction rules for information that has been subject to a preservation notice, once it is no longer subject. We noted in our submission (5.2) that the security principle (NPP4) would apply where the Carrier or CSP was subject to the Privacy Act, and added in oral evidence that this principle includes a requirement to destroy or de-identify personal information once it is no longer needed (NPP4.2). However, as with the security and data quality requirements more generally, we submit that there need to be specific rules in the TIAA about destruction, even though the Convention is silent on the issue of destruction (one of its weaknesses). Specific quality/security/destruction rules are in any case necessary to fill the gap where a CSP falls under the $3million turnover threshold and is therefore exempt from the Privacy Act and its NPPs.

Further submission

In our original submission we said:

> "The CoE Convention has to be read within the context that applies in CoE countries – where there are substantial and actionable constitutional protections for human rights. The absence of any such countervailing protection for human rights in Australia makes it completely untenable for the Convention to be implemented in Australia without very substantial additional provisions that achieve a comparable balance."

One of the additional protections found in all Council of Europe member countries is that they are parties to the Council of Europe Convention on Data Protection (CoE Convention 108), requiring adherence to international standards of data protection. Most are also parties to the Additional Protocol to that Convention, which requires a data protection authority and protection of privacy in data exports. The Convention provides benefits to member states, by guaranteeing that other member states will allow the transfer of personal information to them because they provide international standard privacy protections.

Since 2008 the Council of Europe has actively encouraged non-European states to become members of Convention 108, in much the same way as it encourages non-European states to join the Cybercrime Convention. Uruguay is poised to become the first non-European state to do so.
The Australian Privacy Foundation submits that one of the protections that should be adopted as part of Australia becoming a party to the Cybercrime Convention is that it should also apply to become a

party to Convention 108 and its Optional Protocol. We urge the Committee to recommend that the Australian government seriously consider accession to Convention 108.