Strategy & Corporate Services

Acting Executive Director
Regulatory Affairs
Level 22
275 George Street
BRISBANE QLD 4000
Australia

Telephone (07) 3455 3112

26 July 2011

The Parliament's
Joint Select Committee on
Cyber-Safety
The Secretary of the Committee.
e-mail: jscc@aph.gov.au

Dear Sir/Madam,

I would like to thank you for the opportunity for Telstra to respond to the Inquiry into the *Cybercrime Legislation Amendment Bill 2011.*

Telstra is generally supportive of the proposed amendments to legislation to ensure that Australia is compliant with the Treaty provisions of the European Convention on Cybercrime, including the amendments to the *Telecommunications (Interception and Access) Act 1979 (**TIA Act**),* the *Criminal Code Act 1995* and *Mutual Assistance in Criminal Matters Act 1987.* If passed, these amendments will enable Australian law enforcement agencies to receive requests from and provide assistance to international law enforcement agencies in dealing with online fraud, offences related to child pornography and unauthorised access, use or modification of data stored on computers.

Telstra believes that these proposed amendments will assist in streamlining procedures between carriers and carriage service providers (**C/CSPs)** and law enforcement agencies in the preservation of stored communications. It will also enable C/CSPs to more readily recover the costs incurred when responding to requests from law enforcement agencies.

However, while generally supporting these proposed amendments, Telstra would also like to express its serious concerns that there is no transitional period allowing C/CSPs the time to:

- undertake detailed feasibility studies into these additional obligations;
- design, build and deploy the necessary equipment;
- make network and IT system changes; and
- undertake testing with agencies

in order to be fully compliant with the new legislation.

Making changes to the current practice of preserving stored communications under the "reasonably necessary assistance" provisions of the *Telecommunications Act 1997*[1], as

[1] Section 313, Telecommunications Act 1997.

would be required by the proposed amendments, will require a significant amount of time and financial resources on the part of C/CSPs. Telecommunications networks and systems currently deployed by C/CSPs allow for the preservation of stored communications for a short period of time allowing law enforcement agencies to obtain the necessary warrant. However, under the proposed new provisions, C/CSPs will be expressly required to preserve information for up to **180 days** which will have a major impact on these networks and systems.

In some cases, the existing networks may require significant modifications or even replacement to ensure compliance with such long information preservation periods. Time is required for any such modifications or replacements to be scoped and tested to determine the impacts. Time will also be required for the Lead Agency to provide C/CSPs with the technical information needed to design and build to the network structure required from the proposed new legal framework.

Telstra believes that a reasonable implementation period after Royal Assent and the development of the Lead Agency's handover standard must be provided in order to allow C/CSPs to financially budget for these changes, but also:-

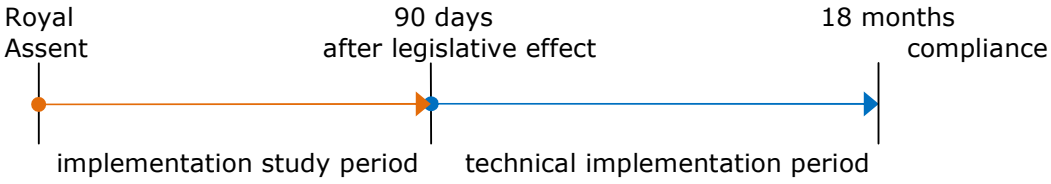
- undertake the necessary feasibility studies to develop technical preservation solutions;
- engage vendors to modify and/or provide additional equipment;
- investigate any new security and privacy risks;
- determine the technical cost impacts on the C/CSP's business;
- build, integrate and test new system and network upgrades to preserve computer and telecommunications data;
- allow the Lead Agency to develop and publish delivery and formatting handover/interface standards (in consultation with industry) for preserved data;
- develop the most appropriate cost recovery model with the Attorney General's Department;
- determine and prioritise additional resources in any existing program of work; and
- allocate additional funding in the C/CSP's budget cycle.

To facilitate the introduction of these proposed amendments and allow C/CSPs to undertake the technical feasibility studies as outlined above, Telstra suggests:-

- an implementation study period of 90 days prior to the legislation coming into effect after Royal Assent; and
- an exemption process for C/CSPs who are unable to comply with the short timeframe, to apply for extra time that may be needed to make the necessary changes to their systems.

We propose the exemption process would require:-

a) the relevant C/CSP to apply to the Communications Access Co-ordinator for an exemption within the 90 day implementation study period;
b) the C/CSP's exemption application to include an implementation plan; and
c) a commitment to implement within a certain period of time after the technical requirements have been published by the Lead Agency, which period would not exceed 18 months.



The 90 day implementation study period would enable the C/CSP to undertake a technical feasibility study into the C/CSP's capability and scope to comply with these enhanced obligations.

Telstra recognises and appreciates that these amendments were made in response to the increasing levels of borderless criminal activity involving computers and the internet but C/CSPs will need time to implement these significant changes to their systems without compromising existing national security and law enforcement activities or in continuing to provide world class telecommunications service to all Australians.

If you or your office require further information, could you in the first instance please contact Michael Ryan on 07 3455 0370

Yours sincerely,

Christine Williams
Acting Executive Director – Regulatory Affairs
Strategy & Corporate Service