Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Cybercrime Legislation Amendment Bill 2011

Alana Maurushat
Lecturer and PhD Candidate, UNSW Faculty of Law
Academic Director, Cyberspace Law & Policy Centre, UNSW Faculty of Law

July 28, 2011

1.0 Introduction

Thank you for the invitation to make a submission on the Cybercrime Legislation Amendment Bill.

This submission is made by researchers at the Cyberspace Law & Policy Centre University of New South Wales Faculty of Law. CPLC is a public interest centre specialising in cybersecurity, cybercrime and the impact of such measures on civil liberties. Alana Maurushat, the Centre's Academic Director, is an expert in the area of Internet Security and Cybercrime, having researched and worked on many pressing cybercrime issues across four continents.

Due to the very short turn-around time from invitation to submit to submission due date, we will limit our submissions into three key areas: 1) highly problematic areas of the Bill, 2) additional measures worth considering and 3) minor problems requiring clarification.

1.0 Highly Problematic Areas of the Bill

I wholly support the ratification of the Convention on Cybercrime and believe that the measures in the Convention are fundamental to combating cybercrime. I am concerned; however, that many of the current proposals go well and beyond the commitments found in the Convention. In some instances, the expansion is necessary to better fight cybercrime but better safeguards are needed to prevent the abusive use of such powers.

Cyberspace Law and Policy Centre
Law Faculty, University of NSW 2052
Ph: +61 2 9385 8027 Fax: +61 2 9385 1778
Email: a.maurushat@unsw.edu.au Web: www.cyberlawcentre.org

1.5 Inadequate Privacy Protection

Expansion of Powers of Privacy Commission:

Currently, the office of the Australian Privacy Commissioner may investigate privacy complaints and resolve them through alternative dispute resolution such as conciliation. Outcomes might include an apology, amendment of records or compensation (monetary or non-monetary). In order to provide solid safeguards for Australian internet users, this process should include enforceability of decisions, such as the power to impose fines on ISPs that breach an internet user's privacy.

Tort of Privacy Invasion:

According to Article 15 of the *Convention,* each party must ensure that the establishment, implementation and application of its powers and procedures be subject to its domestic safeguards for adequate protection of human rights and civil liberties. A tort of privacy invasion should therefore be introduced in accordance with the recommendations of the Australian Law Commission Report on Privacy.

Small Internet Service Providers no longer exempt from National Privacy Principles

Smaller ISPs are classified as "small business operators" who are currently exempt from obligations in the *Privacy Act.* If smaller ISPs are expected to implement real-time interception capabilities and must also preserve data where so compelled, it is critical that they also be bound by the National Privacy Principles.

1.6 There must be Clear Language as to Preservation, Retention and Destruction of traffic data

Title 2 of the *Convention* mandates signatories to adopt legislative and other measures to enable its competent authorities to order the expeditious preservation of traffic data for up to 90 days. However, the *Convention* is silent about the treatment of preserved data after 90 days have elapsed. Any Australian legislative or other measures giving effect to this part of the *Convention* should include clear language as to data retention and destruction.

Preserved data may become a target for information theft. Any person (usually an ISP) preserving traffic data on behalf of a Commonwealth authority should also be compelled to do so subject to a **minimum standard of security**, in order to prevent data breach.

2.0 Additional Measures Worth Considering

While I recognise that the main purpose of the Bill is to ratify the Convention, there are other measures that are required to better combat cybercrime that are neither reflected in this Bill nor the Convention.