NSWCCL
New South Wales Council for Civil Liberties

Postal address: PO BOX A1386 SYDNEY SOUTH NSW 1235
Office address: suite 203, 105 Pitt Street SYDNEY NSW 2000
Phone: 02 8090 2952 Fax: 02 8580 4633
Email: office@nswccl.org.au Website: www.nswccl.org.au

Submission of the

New South Wales Council for Civil Liberties

to the

Joint Select Committee on Cyber-Safety

on the

Cybercrime Legislation Amendment Bill 2011

Renee Watt

1 The scope of this submission is curtailed due to the very limited time for response.

There exists only a very narrow window of time for responding to the Joint Select Committee on Cyber-Safety's ('**Committee**') Inquiry. Further, the materials the Committee has provided for review, which do not include a consolidated version of the would-be legislation, are far from user-friendly. In the result, the New South Wales Council for Civil Liberties ('**CCL**') has only been able to address the *Cybercrime Legislation Amendment Bill 2011* (Cth) ('**Bill**') in part. The CCL has focused on the extraordinary deficiencies in the Bill's approach to the sharing of information obtained under the Bill ('**local information**') with foreign law enforcement agencies ('**requesting bodies**').

The expanded scope of the substantive offences that the Bill proposes may suffer similar deficiencies of over-broad legislation. In relation to the specific offences the Bill proposes, the CCL has not had time to engage with these individually. The CCL therefore makes some high-level comments in this regard, but is unfortunately unable to deal with the technical minutiae of the proposed offences.

2 Summary of recommendations.

In relation to Australia's proposed Bill, the CCL makes the following recommendations:

(a) Australian authorities must *not* disclose *any* local information to a requesting body *unless*:

(i) the disclosure receives the Attorney-General's permission under the **mutual assistance** regime as currently enacted under the *Mutual Assistance in Criminal Matters Act 1987* (Cth) ('**MA Act**');

(ii) further to the current regime, mutual assistance is subject to a court-issued '**mutual assistance warrant**';

(iii) **dual criminality** is satisfied;

(iv) there is no possibility that **torture or the death penalty** will flow from the disclosure;

(v) there is a no danger that the requesting body will **further disclose** the information to another state or a non-governmental authority;

(vi) there is no danger the requesting party will use the information to investigate or prosecute **offences** that are not among the *Council of Europe Convention on Cybercrime*'s ('**Convention**') substantive offences;

(vii) statistics concerning the results of sharing information with a requesting body are among those that Australian law enforcement agencies collect and publish under the Bill; and

(viii) ISPs are obliged to notify subscribers that ISPs may share subscribers' personal information with foreign law enforcement.

Since the Bill addresses none of these points, it will need substantial redrafting before passing into law.

(b) **Data retention** and destruction policies should accompany provisions requiring data preservation.

(c) **Substantive offences** should:

(i) be narrowly drafted so as only to catch dangerous behaviour;

(ii) specifically include botnets; and

(iii) exempt security researchers.

The Bill might help combat cyber-crime, but it will also undermine civil liberties.

2.2 The principle effect of the Bill for Australia will be the sharing of personal information with foreign law enforcement.

At essence, the Bill effects:

(a) Australian/overseas police-to-police-assistance exempt from the current mutual assistance regime under the MA Act and without judicial oversight;

(b) access by foreign law enforcement (via the AFP) to information captured through the domestic warrant system;

(c) data preservation orders; and

(d) State/Federal uniformity of computer-related offences.

2.3 The Bill is a potentially powerful tool for investigators and prosecutors.

Cyber-crime is extremely difficult to police. This principally because:

(a) obfuscation renders trace-back almost impossible; and

(b) cyber-crime tends to be multi-jurisdictional.

By facilitating international cooperation, the Bill addresses one of the two main obstacles in cyber-crime investigations.

2.4 But, as feared, the Bill also powerfully undermines civil liberties.

The CCL holds grave concerns regarding the disclosure of Australian information to foreign law enforcement. Chief among these concerns is that some requesting parties employ torture and the death penalty. Information sharing that results in a person being subject to torture or the death penalty is under no circumstances acceptable. A second significant worry is that covert surveillance of a suspect already comes at the cost of privacy; sharing that information with overseas law enforcement significantly increases the breach of privacy this represents, especially where a regime has comparatively lax standards of privacy or is prone to abuse personal information.

3 The CCL recommends that the Bill be redrafted so as to include the following safeguards to civil liberties.

3.1 Disclosure of local information must be conditional.

The Bill should be amended to include the following restrictions on disclosure of local information to foreign law enforcement:

(a) Disclosure of *any* information to foreign law enforcement must be subject to the current mutual assistance regime.

The MA Act implements a mutual assistance regime that mandates, *inter alia*, the Attorney-General's authorisation before Australian assistance is available to foreign law enforcement. As it stands, the Bill only triggers the current mutual assistance regime in respect of certain categories of information. This is unsatisfactory. To prevent abuse, *all* information provided to a requesting party under the Bill must be subject to the current regime.

That preservation orders are actionable without warrants allows for the timely preservation of volatile evidence. There is no call to circumvent systems in place to prevent civil liberties in the name of timely data preservation.

(b) Further, mutual assistance should be subject to a court-issued 'mutual assistance warrant'.

Just as, before implementing a covert surveillance operation, domestic law enforcement must seek a warrant tailored to the particular circumstances of the operation, so too ought a foreign requesting body be subject to a warrant system that specifically addresses concerns regarding local information in the hands of foreign law enforcement.

A 'mutual assistance warrant' would enable an independent Australian body (the courts) to examine requests for assistance on a case-by-case basis. So as not to place political decisions into the hands of the judiciary, the Bill should list the circumstances to which the court may have regard when deciding whether to issue a 'mutual assistance warrant'. These should include:

(i) whether the applicant has a history of misuse of personal information, such that it seems possible that information collected under the warrant may be:

(A) used to prosecute the suspect for an offence unrelated to the substantive offences the Convention proscribes;

(B) disclosed either to a third country, regardless of whether that country is a signatory to the Convention, or to a non-governmental authority; or

(C) used for any purpose not specified in the application for the warrant;

(ii) whether the applicant employs torture or the death penalty; and

(iii) whether the applicant otherwise has a history of human rights abuses (which concept may require further elucidation).

A 'mutual assistance warrant' should only be required in order for overseas law enforcement to *access* information. In the interests of the timely preservation of volatile evidence, a 'mutual assistance warrant' should *not* be needed for preservation orders.

(c) Dual criminality must be satisfied.

Before Australia shares any information with a requesting body, the offence in pursuit of which the requesting body seeks the disclosure must be an offence, or substantially an offence, under Australian law.

(d) Disclosure should not lead to torture or the death penalty.

The Bill should not allow for the disclosure of local information to a requesting party seeking to investigate an offence that could, if successfully prosecuted, result in torture or the death penalty. Similarly, information should not be disclosed if there is a likelihood of that torture will be employed during resultant investigation.

Where the nation the requesting body represents employs torture or the death penalty for certain offences, Australia should only provide assistance on the undertaking that any information it provides will not be used in a prosecution from which torture or the death penalty may flow. Where under a particular regime torture appears to occur haphazardly, or where Australia does not trust a regime to respect its undertaking, Australia should refuse all assistance.

(e) The requesting body must undertake not to disclose the information to other states or to any non-governmental authority.

Many countries are party to information-sharing agreements and networks. Australia should only share local information if the state to whom the information is to be provided undertakes not to disclose the information to:

(i) any other state; or

(ii) any non-governmental authority, except a court of the requesting state.

Where Australia does not trust a regime to respect its undertaking, Australia should refuse all assistance.

(f) Local information should only be available where the requesting body undertakes to use the information for the sole purpose of investigating and prosecuting cyber-crime.

To avoid the abuse of personal information in the hands of foreign states, Australia should only provide local information where the requesting state undertakes to use the information it receives for the sole purpose of investigating and prosecuting the Convention's substantive offences. The information should not be used for the investigation or prosecution of other offences, including computer-related offences that do not fall within the purview of the Convention's substantive offences.

(g) Statistics should include results of requested information.

Statistics concerning the results of sharing information with a requesting body should be among those that Australian law enforcement agencies will collect and publish under the Bill. That is, whether a request for information by a foreign law enforcement agency has resulted in an arrest, a prosecution, or the charges have been dropped should be publicly available information. This is vital for Australia to evaluate whether information sharing is effective. In particular, if there are many requests but most charges are dropped, we will know that there is a high cost in privacy with a low return in safety.

(h) ISPs should be obliged to notify subscribers that ISPs may share subscribers' personal information with foreign law enforcement.

Because of the Bill's implications for privacy, it should be mandatory that ISPs notify subscribers of the possibility that information regarding their identity and browsing habits could be shared with foreign law enforcement. This should by done by including a warning and explanation in ISPs terms of service and privacy policies. ISPs should be required to notify subscribers of what information the ISPs will gather and share, how they will gather it, and the purpose of this collection.

3.2 Data retention and destruction policies should accompany provisions requiring data preservation.

The Bill allows for foreign law enforcement to request the preservation of significant amounts of data. A vast data repository makes fertile ground for data theft. The Bill must specify security standards attaching to preservation orders. Data retention and destruction policies are essential.

3.3 Substantive offences should be narrowly drafted and tied to serious harm, specifically include botnets and exempt security researchers.

(a) The offences must not criminalise behaviour that is not dangerous.

Any criminal offence should begin with a concept of harm. Harm in cyber-crime can often be difficult to quantify. For example, while the aggregate harm is often enormous, each zombie in a botnet suffers minimal individual harm (see Part 5 below for an explanation of botnets). But difficulties in quantifying harm do not render it permissible to criminalise non-harmful conduct. There is a danger when drafting computer-related offences that in an attempt to capture future technologies the offence is over-broad. Any offence must draw a strong connection between dangerousness and proscribed behaviour. Harm, and particularly *serious* harm, must be retained as an element of the Bill's substantive offences, and should be drafted so as to capture aggregate harm.[1]

(b) The offences must capture botnets.

[1] For a discussion of serious harm in the context of cyber-crime, see Keiran Hardy, 'Operation Titstorm: Hacktivism or Cyber-Terrorism?' (2010) 16(1) *University of New South Wales Law Journal Forum: Cyberlaw*, 31.

Botnets are an example of a criminally-deployed technology that makes use of obfuscation. Put simply, a botnet is a network of compromised computers, usually controlled by a chain of decentralised 'command and control' ('C&C') domain name pages. The compromised computers ('bots', or 'zombies') are infected with malicious software ('malware') usually without a user's knowledge. As one commentator has remarked: "Almost every major crime problem on the Net can be traced to them".[2]

Botnets are the principle technology to enable cyber-crime. There is no specific mention of botnets in the Bill. If the substantive provisions are to be of any use at all, it must be absolutely clear that the creation and deployment of botnets (a collection of compromised computers) is an offence.

(c) Security researchers must be exempt from criminality.

Article 6(2) of the Convention allows for an exemption to criminality where the 'misuse' pertains to security research. It cannot be stressed enough how important this exception is. Currently, security researchers in Australia are not exempt from the computer provisions of the *Criminal Code Act 1995* (Cth). Nonetheless, it is security researchers (university computer science departments, technology companies) that are the primary forces behind tackling botnets and other forms of obfuscation crime tools. There has yet to be a single takedown of a botnet or prosecution of a botnet master that did not involve security researchers. Cyber-crime prosecution cannot occur without their help and they must be free from legal sanction, rather than discouraged from participation.

[2] Scott Berinato, 'Attack of the Bots' (November 2006) *Wired*.