QUEENSLAND COUNCIL FOR CIVIL LIBERTIES
GPO Box 2281 Brisbane 4001
visit us at www.qccl.org.au

Committee Secretary
Joint Select Committee on Cyber-Safety
Department of House of Representatives

**By Email:** jscc@aph.gov.au

Dear Sir,

**RE: Cybercrime Legislation Amendment Bill**

We thank the Committee for the opportunity to make a submission concerning the Cybercrime Legislation Amendment Bill.

Whilst it is stated that

*"No nation alone can effectively combat the problem, it is essential that Australia has in place appropriate arrangements both domestically and internationally to be in the best possible position to combat crime"*

Australia should not pursue this goal as the expense of basic civil and human rights.

The Bill's purpose is to comply with the obligations of the Council of Europe's Convention on Cybercrime. We attach a copy of our submission to the Attorney General on Australia's accession to the convention. We summarise our principal objections to Australia's accession.

## 1. Problems with the convention

### 1.1 Potential Signatories

Countries with human rights records described as "poor" in the most recent US Country Reports of Human Rights Practices have already signed and ratified. For example the Ukraine has signed and ratified, and yet Canada, Japan and the UK have signed but not ratified. As a result of this Bill Australia may be cooperating with governments whose civil liberty histories are questionable at the least – countries in which police have been known to torture and kill people in the course of their "investigations".

## 1.2 Mutual Assistance

Whilst it is true that the convention does allow the cooperating nation to refuse to investigate any crime that is a "political offence" the term "political offence" is not properly defined in the convention so this does little to protect Australia from becoming a useful tool in the politically motivated actions of another country. For example, the Ukraine in the past has often used criminal libel and defamation laws to suppress dissent and press freedom. Under the "Mutual Assistance", Australia would be forced to cooperate with the Ukraine despite the fact that the information provided could be used for political motives against our democratic principles.

## 1.3 Definition of Cybercrime

The following are just a few actions that might fall into the category of Cybercrime according to the convention:

- The prank of taking someone's mobile phone and changing their ring tone to something embarrassing before giving it back.
- The posting of comments on a forum or blog which the site owner had prohibited.
- Since most phones are now 'smart' and many calls now travel over the internet, the distinction between these laws and phone tapping laws is becoming nil.
- Reading someone's computer screen over their shoulder or reading someone's text messages off their phone.
- Scanning for a WiFi connection (a free or public one) and picking up the existence of others in the area.
- Possession of many tools used by IT professionals to assess the security of their own or client's networks. It could make authors of such software liable if it were misused by others.
- Voting twice in an online poll e.g. Courier Mail polls

Before moving on to the issues with the actual Bill there are 2 vital things that the convention itself lacks. They are:

## 1.4 Lack of Dual Criminality Provision

What is missing and certainly required is an article requiring that, prior to one country demanding cooperation from the other, the offence be a criminal

offence in both countries. The Bill seeks to address this but not adequately in our submission.

### 1.5 Lack of Transparency

The Convention makes no allowance for transparency and accountability. There is no requirement in the convention that any individual ever be informed that he or she were the subject of government scrutiny. This leaves citizens with no means of challenging any determinations made under the convention. The Bill provides no device for addressing this.

## 2. The Bill

The following are a list of the offensive sections of the Bill:

### 2.1 Section 15B of the Mutual Assistance in Criminal Matters Act 1987

This section states that Australia may respond to a foreign country's request for access to stored information for foreign law enforcement purposes. It will enable the Attorney General to authorise the AFP or state police to apply for a stored communication warrant under section 110 of the TIA Act if:

- A request for access to the stored communications has been received from the foreign country
- An investigation or interrogative proceeding into a criminal matter has commenced in the requesting country
- The offence the subject of the investigation or investigative proceeding is punishable by a maximum penalty of three or more years imprisonment, life imprisonment or death or a fine equivalent to or greater than 900 penalty units
- There are reasonable grounds to believe that a carrier holds stored communication relevant to the investigation or investigative proceedings.

The issues with this section are twofold:

1. Point 2 refers to the necessity that a criminal matter has already been commenced in the foreign country. This is problematic in the sense that each country has different criminal procedures. The recent Julian Assange case illustrates one of the difficulties caused by differences of procedure. In our view, individuals should not be deported purely for the purposes of questioning. In this context the process in the foreign country should be required to have at least reached the stage that would justify the issue of a warrant under our laws.

2. The third point makes it necessary that the offence be a "serious" offence in that country including the possibility of death. We should not be assisting in the investigation of a capital offence.

## 2.2 Part IIIB of the Mutual Assistance in Criminal Matters Act 1987 (Assistance in Relation to Telecommunications Data)

Subsection 15D(2) will set out when the Attorney General can authorise the provision of assistance to a foreign country. The Attorney General will only be able to make an authorisation if satisfied that:

- An investigation relating to a criminal matter involving an offence against the law of the foreign country (the requesting country) has commenced in the requesting country and

- The offence to which the investigation relates is punishable by a maximum penalty of imprisonment for three or more years, imprisonment for life or death penalty.

It is stated that
"*The penalty threshold of three years imprisonment mirrors the threshold that applies to accessing prospective telecommunications data for domestic purposes*".

Whilst this may appear true on paper, the reality is that an offence with a maximum penalty of 3 years in any given country may not be the same offence or even an offence at all in Australia.

## 2.3 Section 5EA of the Telecommunications (Interceptions Access) Act 1979

This new section will define serious foreign contravention in the same wording as that of Section 15B (as previously discussed) of the Mutual Assistance in Criminal Matters Act 1987. The issues regarding this section are the same as previously mentioned.

## 2.4 Section 6DB of the Telecommunications (Interceptions Access) Act 1979

This section defines an *Issuing Authority* as:

- A judge of a court created by parliament who has consented to being appointed an issuing authority

- A federal magistrate who has consented to being appointed an issuing authority

- A magistrate who has consented to being appointed an issuing authority

- A member, senior member or Deputy President of the AAT who is enrolled as a legal practitioner and has been enrolled for at least 5 years.

The Council takes the opportunity to restate it's longstanding objection to the AAT being given powers to issue warrants. Members and Deputy Presidents of the AAT do not have the status of judges and accordingly are not sufficiently independent to be exercising this most important of powers authorising violation of some of the most basic civil rights.

## 2.5 Subsection 116 (2A) of the Telecommunications (Interceptions Access) Act 1979

Under this section will be listed the factors that will need to be considered if the stored communications warrant application is a mutual assistance application. These factors include:

- How much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant

- The gravity of the conduct constituting the serious foreign contravention and

- How much the information that would likely be obtained through accessing the stored communications would be likely to assist in connection with the investigation.

The difficulty with this proposal is that it is too vague. Which standards are used to make this decision? It is proposed that an interference with a person's privacy would be interpreted more broadly than those situations outlined in the Privacy Act 1988 but exactly how broad is unknown.

It is stated:

*"This will ensure that each warrant application is determined by reference to specific criteria and not irrelevant matters."*

However the criteria are NOT specific in the sense that the degree of interference with someone's privacy is not specifically outlined anywhere.

The phrase "likely to assist in connection with the investigation" is likewise an immeasurable reference. Virtually anything can be classed loosely as being connected to any particular investigation. As such this leaves too much discretion to the authority and much potential for abuse.

## 2.6 Subsection 116 (1)(d) of the Telecommunications (Interceptions Access) Act 1979

This section is to be amended to read that an issuing authority may issue a stored communications warrant if satisfied that information likely to be obtained pursuant to a stored communications warrant will be likely to assist with:

- The investigation of a serious contravention domestic offence, or
- The investigation by a foreign country of a serious foreign contravention.

Again we are confronted with the same issue. What may be defined as a serious contravention in one country may be perfectly legal or de-criminalised in Australia. The Bill makes no allowances for this.

The same arguments can be made for sections 116(3) and 118 of the Act.

## 2.7 Section 142A of the Telecommunications (Interceptions Access) Act 1979

This section will set out the conditions that must be complied with in communicating information obtained under a stored communications warrant to a foreign country.

These conditions are:

> That the information will be used for the purposes for which the foreign country requested the information
>
> That any document or other things containing the information will be destroyed when it is no loner required for those purposes and
>
> Any other conditions determined in writing by the Attorney-General.

This is all very well in theory but the difficulty in practice of this section is its enforceability. Once information is released to a foreign jurisdiction we have no way of monitoring, enforcing or regulating exactly what happens to the information once provided. For this reason stringent safeguards need to be in place prior to the release of information. The Bill fails to provide those safeguards.

## 2.8 Section 180 (3) of the Telecommunications (Interceptions Access) Act 1979

This section will set out when an authorised officer is able to make an authorisation under ss180(2) . An authorised officer will only be able to make an authorisation if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country.

This is another point at which there should be in the Bill a requirement of dual criminality as this should not be simply judged by the period of time that a person can be imprisoned for being convicted of the offence.

## 2.9 Section 180F - of the Telecommunications (Interceptions Access) Act 1979

This section will require an authorised officer prior to making an authorisation, to have regard to how much the privacy of any person or persons would likely be interfered with by the disclosure.

However what level of interference with a person's privacy that might be unacceptable is not defined nor are any standards alluded to for reference.

## 2.10 Section 180(3)(B) of the Telecommunications (Interceptions Access) Act 1979

States that the Attorney-General will only be able to make an authorisation under section 15D of the MA Act if satisfied that:

- An investigation relating to a criminal matter involving an offence against the law of the foreign country has commenced in that country
- The offence to which the investigation relates is punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty.

This is inadequate in the sense that an offence under prosecution in any particular country cannot be the basis of decision making in Australia unless the legislation applicable to that offence is exactly the same in Australia. Otherwise we are giving other jurisdictions permission to deal with citizens in ways we would not contemplate here.

## 2.11 Criminal Code Act 1995 - Serious computer offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

*Intention to commit a serious Commonwealth, State or Territory offence*

(1) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or
(ii) any unauthorised modification of data held in a computer; or
(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a carriage service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

It is proposed that in s4771(1)(b) that the words carriage service be changed to read "that are not limited to carriage services". This broadens the use of the section to cover interferences such as those listed earlier on this submission making it possible for virtually anything to become a Cybercrime.

## 3. Public Interest Monitor

The Council has a longstanding concern about the number of warrants issued in this country.

For example, in the twelve months 2004 – 2005 there were 2,883 warrants issued in Australia. In the twelve months of 2005 US Courts issued 1,774 warrants. In raw figures alone Australia issued 63% more warrants than the US. Adjusting for population Australia intercepts telephone communications 24 times more per capita than the United States. The position has worsened. The Federal Attorney General's Annual Report for 2009 – 2010 shows that 3,589 phone taps were approved in Australia and only 5 requests were refused.

Phone tap applications are made in Australia in closed courts – the only people present being the judge and the representative of the police providing the judge with no alternative point of view. In the mid 1990's the conservative Borbidge government introduced into Queensland the Public Interest Monitor ("the PIM"). The Public Interest Monitor and his or her deputy are barristers in private practice who appear before Supreme Court Judges on applications for listening devices. When Queensland law enforcement agencies are seeking a phone tap they must notify the PIM who then appears before the Judge who hears the application. The result is that phone tap applications in Queensland are no longer one sided with the PIM being able to cross examine the police and make submissions to the judge.

This innovation has been welcomed by Queensland judges.

We are aware that the Senate National Crime Authority Committee's Report *Street Legal* rejected the introduction of a PIM. That rejection was in relation to authorising controlled operations not warrants. In any event it is our submission that none of the criticisms made by that committee, which took evidence only a few years after the introduction of the PIM in Queensland, have been vindicated by subsequent experience.

It is the Council's submission that the powers of Federal Ombudsmen are not, despite the opinion of that committee, a sufficient safeguard.

It is important to remember that the powers proposed under this legislation may result in the prosecution of individuals, be they Australian citizens or not in foreign countries. Those individuals will more than likely have no effective form of redress in an Australian Court. It is important therefore that all steps possible are put in place to prevent the misuse of this legislation by foreign governments.

Even with the introduction of the Public Interest Monitor it would be the Council's view that the legislation will be fundamentally floored and should be rejected. However, the introduction of a Public Interest Monitor would at least go some way to ensuring that a Court or tribunal hearing an application for a warrant under this legislation has the prospect of having maximum possible range of issues ventilated before it.

**Summary**

In our submission the Bill ought to be rejected. In a context where the result of a decision under the legislation will be almost entirely beyond redress in an Australian Court the Bill provides inadequate protection for human rights.

This submission is primarily the work of Tina Riveros with input by Andrew Sinclair and Michael Cope.

Yours faithfully,

Michael Cope
President
For and on behalf the
Queensland Council for Civil Liberties
25 July 2011

QUEENSLAND COUNCIL FOR CIVIL LIBERTIES
GPO Box 2281 Brisbane 4001
visit us at www.qccl.org.au

Assistant Secretary
Telecommunications and Surveillance Law Branch
National Security Law and Policy Division
Attorney-General's Department
3 – 5 National Circuit
BARTON ACT 2600

28 February 2011

**RE: AUSTRALIAN'S PROPOSED ACCESSION TO THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME**

Dear Assistant Secretary,

We recommend that you do not accede to the Council of Europe Cybercrime Convention in its current form due to the potential threat it poses to International Human Rights.

We refer to your public consultation documents and note that you identify the reason for establishment of the Council of Europe "the protection of human rights, democracy and the rule of law." Upon inspection of the convention, it is the case that in fact several aspects of the convention are in direct conflict with this purpose as they allow for the deterioration of some fundamental human rights and democratic freedoms.

The following are a list of those offensive sections of the convention:

1. **Potential Signatories**

   Article 36 (1) states: "This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration."

   Article 37 (1) states "After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers."

   Given that the signatories are not limited it is already the case that countries with human rights records described as "poor" in the most recent US Country Reports of Human Rights Practices have already signed and ratified. For example the Ukraine has signed and ratified, and yet Canada, Japan and the UK

have signed but not ratified. If Australia signs and ratifies and other countries are invited to do the same Australia can be forced to cooperate with governments whose civil liberties practices are questionable at the least – countries in which police have been known to torture and kill people in the course of their "investigations".

**2. Mutual Assistance**

Article 25 (1) states: "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." Whilst it is true that the convention does allow the cooperating nation to refuse to investigate any crime that is a "political offence" the term "political offence" is not actually properly defined in the convention so this does little to protect Australia from becoming a useful tool in the politically motivated actions of another country. For example, the Ukraine in the past has often used criminal libel and defamation laws to suppress dissent and press freedom. Under the "Mutual Assistance", Australia would be forced to cooperate with the Ukraine despite the fact that the information provided could be used for political motives against our democratic principles.

**3. Criminalisation of Certain Offences**

Articles 2 – 11 require that the specified offences are transposed as crimes into Australian Law. It requires that offences, such as hacking; the production, sale or distribution of hacking tools and offences relating to child pornography be criminalised as well as expanding the already existing criminal liability available for intellectual property violations. The scope of the criminality for computer-related crimes is too broad and in actual fact covers more than just "computer related crimes". By definition virtually any crime may become a cyber crime – for example: Even a robbery committed by criminals using a wireless email device would be a "cyber crime". Some examples serve to illustrate how a wide reading of the convention could oblige Australia to criminalise things that would seem quite surprising to most voters.

They could apply to the prank of taking someone's mobile phone and changing their ring tone to something embarrassing before giving it back.

They would arguably include anyone posting comments on a forum or blog which the site owner had prohibited.

Since most phones are now 'smart' and many calls now travel over the internet, the distinction between these laws and phone tapping laws is becoming nil.

Article 2 could seem to cover reading someone's computer screen over their shoulder or reading someones text messages off their phone.

Article 3 could seem to make illegal even scanning for a WiFi connection (a free

or public one) and picking up the existence of others in the area.

Article 6 could make the possession of many tools used by IT professionals to assess the security of their own or clients networks an offence. It could make authors of such software liable if it were misused by others.

Article 14 - There is an underlying assumption that the convention will be used to force internet service providers to record and keep and presumably retrieve on demand, massive amounts of data about their customers. This is technically challenging and expensive. It's also very easy for any decent criminal or terrorist to get around so would result in the recording of massive amounts of data about everyone in the off chance it included some about someone of interest.

**4. Lack of Dual Criminality Provision**

What is missing and certainly required is an article regarding dual criminality. This article should make it a requirement that, prior to one country demanding cooperation from the other, the offence be a criminal offence in both countries. Without this, it is the case that Australian Law Enforcement would be required to cooperate with foreign police forces in their investigation of offences that in Australia are not considered a crime at all.

**5. Lack of Transparency**

The Convention makes no allowance for transparency and accountability. There is no requirement in the convention that any individual ever be informed that he or she were the subject of government scrutiny. This leaves citizens with no means of challenging any determinations made under the convention. In a country that values transparency and accountability as an important means of maintaining the existence of the rule of law, this lack of possibility of review is in direct contradiction of our fundamental values. The convention also flies in the face of the current requirements for use of interception legislation in Queensland which require the involvement of the Public Interest Monitor.

**6. Inadequate safeguards**

Article 15 (Conditions and Safeguards), provides, inter alia, that each party must ensure that "the establishment, implementation, and application of the powers and procedures provided for in this Section [Procedural Law] are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties." This provision is quite vague, and is not reiterated with specific and detailed protections within any of the specific provisions. For example, provisions on expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data make no mention of limitations on the use of these techniques with an eye to protection of privacy and human rights.

In your public consultation document it is stated that "Australia has specific laws targeting cyber crime, including offences targeting unauthorised access, modification

of computers or computer systems, online child exploitation. Online copyright infringement and online fraud."

It further states, "Australian law also provides law enforcement agencies with appropriate powers to properly investigate and prosecute cyber crime: Including powers to utilise telecommunication interception and surveillance devices."

Given the existence of these apparently useful protections in the current law, is it really necessary to enter the convention, a convention that purports to: curb important civil liberties by limiting accountability; further criminalising certain computer related offences and risking Australia being forced to support the human rights infringements of other nations? The Council notes that the material provided contains no justification in terms of case studies, statistics or even potential examples of where the existing laws or international cooperative arrangements have caused a problem for Australia or for any EU country in adequately enforcing their existing laws.

Of even greater concern is that to properly implement the convention would require substantial changes to our law. This is despite the claim 'Australia is compliant with this article' in many cases. Clearly the Australia version of the law is only a subset of what is possible. To accede to the Convention would be to encourage law enforcement agencies to argue for an increase in powers or offences when none is currently justifiable.

We submit that on the balance, the potential benefits of entering the convention (which are few given that many of the issues raised by the convention are ones already well legislated and regulated within Australia) are far outweighed by the risk we face in signing and ratifying leaving us essentially bound to use extraordinary powers to engage in less than democratic political investigation for other countries whose values we do not share as a nation.

This submission was the work of Council member Tina Riveros with input from Vice President Andrew Sinclair.

We trust this is of assistance to you in your deliberations.

Yours faithfully

Michael Cope
President
For and on behalf the
Queensland Council for Civil Liberties
14 March 2011

MJC:MJC:2050882_970.doc