Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

26 July 2011

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

Dear Senator Bilyk

Re: Cybercrime Legislation Amendment Bill 2011

The attached Submission from the Australian Privacy Foundation concludes as follows:

- the Bill has been placed before the Parliament in a manner that obstructs understanding of its meaning and analysis of its impacts
- the Bill seeks to impose all of the intrusive elements of the Convention without allowing for the Convention's presumption that strong human rights protections are in place. As a result, its provisions would create grossly unbalanced and excessive legislative powers
- despite its claimed purpose, the Bill goes well beyond what is necessary in order to accede to the Convention, and the extensions are highly privacy-abusive
- despite the barriers to understanding, the APF has identified many serious features that should under no circumstances be passed into law
- the Bill very probably contains further excessive features that cannot be readily detected because of both the inherent and contrived complexities in the material provided
- the APF submits that the Committee must find that, in its present form, the Bill is completely unacceptable, and incapable of amendment into an acceptable form

In the last decade alone the Australian Parliament has enacted some 50 statutes containing highly intrusive and in many cases unjustified measures, on the basis of mere assertions by national security and law enforcement agencies, and in the face of explicit and carefully reasoned opposition from public interest advocacy organisations and much of the legal profession.

The APF calls on the Joint Select Committee use the opportunity of this Inquiry to make a stand and start reversing this recent trend, which threatens a free society. You should 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 proposed amendments.

For your information, the APF Board SubCommittee that prepared this Submission comprised Dr Mark Burdon of the University of Queensland Law School, Dr Roger Clarke, Visiting Professor in the ANU Research School of Computer Science and the UNSW Faculty of Law, and Mr Nigel Waters, former Deputy Privacy Commissioner and Visiting Fellow at the UNSW Faculty of Law.

Yours sincerely

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

Australian Privacy Foundation

Submission to the Joint Select Committee on Cyber-Safety

Inquiry into Cybercrime Legislation Amendment Bill 2011

1. The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. Further information is attached, and at www.privacy.org.au. APF has made significant contributions over the last 15 years to the development of telecommunications interception and access legislation – as acknowledged in many of the reports of the Senate Legal and Constitutional Affairs Committee, which has historically been the Committee which reviewed Bills to amend this legislation.

2. Cybercrime

Society wants protections against criminal behaviour, and it is important that national security and law enforcement agencies have means available to them to combat 'cybercrime'.

That term is not defined in the Convention, the Bill, the Explanatory Memorandum or the Acts that the Bill seeks to amend, nor even in the Cybercrime Act 2001. Presumably it represents the sum of the sub-areas addressed in Articles 2-10 of the Convention; namely illegal access to computer systems, illegal interception of non-public transmissions between computer systems, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offence related to the handling of child pornography using computer systems, and offences related to infringements of copyright and related rights. With the exception of the last, which has only recently become a matter of criminal law – this 'package' is very similar to the longstanding concept of 'computer crime'.

Cybercrime is a threat to people's welfare. It has significant negative impacts on privacy. The APF is accordingly supportive of laws that will demonstrably assist in addressing cybercrime, provided that the collateral harm that they cause is commensurate with their benefits, and the powers that they confer are measured and controlled.

3. The CoE Convention and Human Rights

The APF has followed the emergence of the Council of Europe (CoE) Convention on Cybercrime over the last 15 years. Although the Convention began as a seriously excessive log of claims, it was progressively pared back to a more balanced document. APF's international counterpart, Privacy International, was active in the arduous consultative processes that ensured that the draft Convention's early extremism was considerably tempered prior to its completion.

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.

National security agencies and law enforcement agencies have a natural tendency to 'overreach' in seeking and using powers which can, if misused, represent serious threats to democracy. This is partly because of the clandestine manner in which they operate, the strong tendency of some of their executives to regard their judgement as being superior to that of Parliament and the Executive, and the substantial and inadequately controlled powers that they already enjoy.

It is accordingly critical that the Parliament consider very carefully every attempt by these agencies to garner additional and enhanced powers. The criteria that the Parliament must apply include:

- justification, not mere assertion, of the need for the powers that are sought

- transparency of purpose, of the measures, of the processes and of the outcomes
- explicit scope of the powers, and unambiguous constraints on the powers
- *ex ante* controls over the use of the powers
- *ex post facto* controls over the use of the powers
- independent and transparent reporting, monitoring and oversight
- explicit and enforced criminal sanctions for mis-use and abuse of the powers

4. Process Aspects Relating to the Bill

The process that has led to the submission of the present Bill to the Parliament began very badly. As we said in our Supplementary Submission to the Senate Standing Committee on Environment, Communications and the Arts Inquiry into the Adequacy of Protections for the Privacy of Australians Online on 30 November 2010, at http://www.privacy.org.au/Papers/Sen-OLP-Sub2-101130.pdf :

> "In April 2010, the Government announced its intention to accede to the European Convention on Cybercrime. This was done without consultation with civil society, and without adequate consideration of personal data security and privacy risks. Even the US baulked at aspects of the Convention, and Canada has adopted a much more sceptical view".

Further, the APF's contributions to the process have been severely hampered by the failure of the Attorney-General's Department to ever discuss the matter with the APF, or to at any stage provide the APF with an opportunity to provide a submission to it (although we understand that some other organisations were afforded that opportunity). Nor was the APF invited to provide evidence by the Joint Standing Committee on Treaties.

Moreover, **the process surrounding the review of the legislation by this Committee has been in direct conflict with the reasonable expectations of civil society**. In particular:

- an impossibly short period was made available to consider complex, highly unclear and highly intrusive draft legislation. This undermines the capacity of NGOs to give proper consideration to the Bill, and to confidently provide evidence to the Committee, and undermines the Committee's capacity to give proper consideration to views other than those of the Department.

  The APF received a formal invitation to submit on Friday 8 July, advising a submission date of Friday 15 July. On Wednesday 13 July, the APF received an invitation to present evidence to the Hearings, to be held exclusively in Canberra, on Tuesday-Wednesday 19-20 July.

  The provision of a mere 5 business days severely disadvantages public interest advocacy organisations. The practicalities of organisations that depend on volunteer hours from busy professionals, that endeavour to assess proposals thoroughly, that prepare and review text carefully, and that operate in a collegial and consultative manner, demand a minimum period of notice in a case such as this of 25 not 5 days.

  The extension of 7 business days to 26 July was advised only as the impossible deadline of 15 July passed
- no document appears to have been provided that traces the development of policy to accede to the Convention, through the Attorney-General's Department and previous Parliamentary Committees. It is therefore unclear to what extent the Bill does and does not reflect prior submissions, discussions and undertakings.

  As a result, each civil society organisation has been forced to re-commence the evaluation from the beginning – which is a horrendous waste of resources in any circumstances, but much worse given their voluntary nature.
- no consolidated statutes have been provided, to show the textual effect that the amendments would have if passed.

  Particularly with such complex legislation, this is essential as a tool for the analysis of the amendments' meaning and impacts. With current technologies, consolidated statutes are not

difficult to produce, and it is reasonable to assume that in a legally professional context such as the Department, they have already been produced for internal use.

5. Some Clearly Unacceptable Features of the Bill

The stated purpose of the Bill is "to ensure that Australian legislation meets all the Convention's requirements" (Explanatory Memorandum para 1).

However, as the evidence below demonstrates, **the Bill goes well beyond its stated purpose**. The APF interprets this a yet another attempt by the national security and law enforcement interests to exploit an opportunity to gain powers that are far wider and deeper than those that accession to the Convention requires. **The passage of this Bill would have a serious and unjustified detrimental impact on the privacy of Australia citizens.**

In the short time made available, the APF has identified the following aspects of serious concern:

- extensions to the scope of the Bill
- inadequate obligations concerning he security and integrity of preserved data
- grossly inadequate privacy protections
- inadequate implementation of the 'Dual Criminality' principle

Our main comments in this section of the submission relate to Schedule 1 of the Bill which introduces a preservation and access mechanism for stored communications, as defined in the TIAA, and to Schedule 2 which provides for mutual assistance with other countries.

5.1 Extensions to the Scope of the Bill

Several of the Bill's key elements are drafted in a manner that extends the scope of Telecommunications (Interception and Access) Act 1997 (TIAA) regime, with negative impacts on privacy far in excess of that which could be argued to be needed in order to achieve mere 'accession to the Convention'.

5.1.1 The Scope of 'Stored Communications'

The Convention recognises the privacy sensitivities arising from the preservation and collection of stored computer data and makes a clear delineation between 'traffic data' and the content of communications. Regarding preservation, Article 16(1) states

> Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

Article 17(1) then goes on to specify the instigation of specific measures in relation to the expedited preservation and partial disclosure of traffic data.

Regarding collection, Article 20 requires Parties to legislative measures to collect or record traffic data or to compel a service provider, within its existing technical capability to confidentially collect, record or assist a Party to collect or record, real-time traffic data.

Article 21 refers to the interception of content data which can only be intercepted in relation to a range of serious domestic law offences. The interception of content data accordingly has a higher test than the collection of traffic data, namely, in relation to a serious domestic law offence, principally due to the privacy sensitivities arising from the nature of content data. These points are set out clearly in the Convention's Explanatory Memorandum.

> 209. The type of data that can be collected is of two types: traffic data and content data. 'Traffic data' is defined in Article 1 d to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).
>
> 210. In many States, a distinction is made between the real-time interception of content data and real-time collection of traffic data in terms of both the legal prerequisites required to authorise such investigative measure and the offences in respect of which this measure can be employed. While recognising that both types of data may have associated privacy interests, many States consider that the privacy interests in respect of content data are greater due to the nature of the communication content or message. Greater limitations may be imposed with respect to the real-time collection of content data than traffic data. To assist in recognising this distinction for these States, the Convention, while operationally acknowledging that the data is collected or recorded in both situations, refers normatively in the titles of the articles to the collection of traffic data as 'real-time collection' and the collection of content data as 'real-time interception'.

Accordingly, the collection and use of traffic data can provide significant evidence of criminal behaviour without the intrusiveness of intercepting an individual's actual communication. The Memorandum therefore recognises that there are greater privacy sensitivities arising from content data and some existing domestic laws have higher legal standards regarding the collection and interception of such information. However, the Memorandum also goes on to recognise

> 211. In some States existing legislation makes no distinction between the collection of traffic data and the interception of content data, either because no distinction has been made in the law regarding differences in privacy interests or the technological collection techniques for both measures are very similar. Thus, the legal prerequisites required to authorise the undertaking of the measures, and the offences in respect of which the measures can be employed, are the same. This situation is also recognised in the Convention by the common operational use of the term 'collect or record' in the actual text of both Articles 20 and 21.

The question therefore arises whether the Bill should specifically acknowledge the difference between traffic and content data. We contend that it should.

As currently drafted, the Bill does not specifically differentiate between traffic and content data and instead merely refers to "stored communications" which is not defined. The use of this phrase is unnecessarily broad and increases the scope for unwarranted privacy intrusions into personal communications where preservation and disclosure of traffic data alone could be sufficient in terms of an ongoing criminal investigation. Australian telecommunications and interception law already clearly distinguishes content and other data, with different thresholds, test and controls for collection and recording, and there is no excuse for not reflecting this distinction in the current Bill.

We contend therefore that the Bill should clearly distinguish between traffic and content data for the purposes of preservation and collection, and stricter controls should apply to the preservation and interception of content data.

A Bill to enable accession to the Cybercrime Convention must:

- **reflect the clear distinction between traffic and content data for the purposes of preservation, and any subsequent collection and disclosure**
- **ensure that the much higher threshold tests and stricter controls regarding activities that involve content data are not compromised in the new preservation and access regime**

5.1.2 The Scope of 'Telecommunication Services'

The Bill would create three types of preservation notice that would generally require a carrier to preserve for the duration of a notice all stored communications that relate to the person or the telecommunications service specified in the notice. Telecommunications service is not defined in the Bill and therefore the default definition is found in s5 of the TIAA.

> ***'telecommunications service'*** means a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication

In the existing TIAA, it is implicit that any interception or access to stored communications must only occur in relation to specified individuals (or accounts) – warrants cannot be issued for 'all accounts' or even a block of accounts. In the new context of preservation notices it is not clear if this welcome constraint will apply. A serious problem may arise in the construction of "relate to the person or telecommunications service specified in the notice". Preservation notices could arguably be issued in relation to a telecommunications service, being an account type offered to a number of individuals. This point is re-emphasised in what the agency can specify in a notice:

(a) One person; or

(b) One or more telecommunications services; or

(c) One person and one or more telecommunications services.

As highlighted, sub-clause (b) is particularly problematic because if it can include a service or services provided to numerous individuals. This could lead to the unnecessary preservation of thousands of records with the possibility of further disclosure. The construction of the notices could consequently lead to the preservation of entire data sets, which could then be used for 'fishing expeditions' which is clearly contrary to the purpose of the Convention, as exemplified in the Explanatory Memorandum regarding the collection of traffic data.

> 219. Under this article, the traffic data concerned must be associated with specified communications in the territory of the Party. The specified 'communications' are in the plural, as traffic data in respect of several communications may need to be collected in order to determine the human source or destination (for example, in a household where several different persons have the use of the same telecommunications facilities, it may be necessary to correlate several communications with the individuals' opportunity to use the computer system). The communications in respect of which the traffic data may be collected or recorded, however, must be specified. Thus, the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.

The Explanatory Memorandum states that for the purposes of an investigation it may be necessary to collect communications data from different persons (e.g. a household) but the traffic data collected must be specified. In the context of the Bill, a preservation notice will precede collection and we contend that the same principles should be applied to preservation notices as well as subsequent disclosures.

A Bill to enable accession to the Cybercrime Convention must:

- **in terms of stored communications, "(a) relate to the person *and a specified telecommunications service or services*" and**
- **in terms of what an agency can specify, "(a) *one person and one or more specified telecommunications services used by the person who is subject to this notice*"**

- **make it clear that 'telecommunications service' does not include a service provided to a class of customers**

The effect of these changes will diminish the prospects of fishing expeditions in preservation notices by restricting the preservation of communications data to one individual and/or one telecommunications service (being a single 'account').

Finally, the breadth of the current construction of preservation notices again re-emphasises the need to delineate between traffic and content data. As it stands, the Bill could require an Internet Service Provider to preserve all stored communications (e.g. traffic and content data) for a telecommunications service (e.g. email, text messaging, mobile phone) for a specified period of time. Unless our concerns about the meaning of a 'service' are addressed, then under an ongoing domestic preservation notice, a Commonwealth agency could arguably request that a major carrier such as Telstra or Optus, preserve *all* emails used on its service for a 30 day period. Such a notice could cover hundreds of thousands of customers, and millions of communications and would be wholly unacceptable. It would also pre-empt any reasoned consideration of a statutory data retention requirement (see 5.3 below).

If it is not the government's intention to allow preservation orders to cover 'bulk' data, then this needs to be made unequivocally clear in the Bill.

5.1.3 The Scope of 'Issuing Agency' under s107H

Under s107H(1), an issuing agency may give a domestic preservation notice that requires a service carrier to preserve all stored communications relating to (a) a person or service specified in the notice and (b) the data the carrier holds at any time following receipt of the notice. An historic domestic preservation notice requires a carrier to preserve communications held by a carrier on the day of the notice for up to 90 days in order to assist the issuing agency to gather intelligence in relation the contravention of a certain Australian law. An ongoing domestic preservation notice requires a carrier to preserve communications held by a carrier for a 29 day period after the carrier has received the notice.

An issuing agency is defined unhelpfully under s5(1) as "in relation to a preservation notice means, the agency that gives the notice".

There are two types of issuing agency:

- an enforcement agency that can instigate an historic domestic preservation notice; and
- an interception agency that can instigate an ongoing domestic preservation notice.

The term 'enforcement agency' is not defined in the Bill and the definition of s5 of the TIAA applies – which broadly refers to law enforcement and anti-corruption authorities.

On the other hand, s7 of the Bill defines an interception agency, for the purposes of Part 3-1A, as:

(i) a Commonwealth agency; or

(ii) an eligible authority of a State in relation to which a declaration under s34 [of the TIAA] is in force.

This seems inconsistent with the statement in the Explanatory Memorandum (page 5) that "…an issuing agency (which is an enforcement agency or the Organisation)..." (or for foreign notices only the AFP).

It is well beyond a reasonable interpretation of the Convention to give *all* Commonwealth agencies access to the new preservation powers, particularly in relation to the broader scope of ongoing domestic preservation notices, and we therefore question the provisions of the Bill that appear to do this, contrary to the explanation in the EM. In any event, the term 'interception agency' should not be used in a way that is either inconsistent with its use elsewhere, or misleading or confusing.

It is essential that a Bill to enable accession to the Cybercrime Convention strictly limits the range of agencies that can issue preservation notices to those which are authorised to subsequently exercise access powers.

5.1.4 Extensions to the Scope of 'Foreign Countries'

The Bill (and the Explanatory Memorandum) refer to 'foreign countries' with reference to the instigation of a foreign preservation order. The term 'foreign countries' is not defined and it is capable of very wide interpretation, including for example states that are not parties to the Convention.

One of the benefits of the Convention is that it establishes formalised legal mechanisms for co-operation in cybercrime investigations whilst ensuring that important societal balances, including privacy, are considered. Non-parties to the Convention obviously would not have to consider these important issues. As the basis for implementing the Bill is to accede to the Convention, it is unacceptable for non-parties to the Convention to be allowed to cause the preservation of, and possibly acquire, stored communications about Australian and foreign nationals in Australia.

We note that as of this month, only 4 non-Council of Europe countries have signed the Convention and that of those, only the US has ratified it (taking effect in 2007). This means that the vast majority of countries that might seek preservation and/or disclosures under the proposed new provisions of the TIAA would not be party to the Convention and its conditions and safeguards.

It is essential that a Bill to enable accession to the Cybercrime Convention not encompass all 'foreign countries'. The provisions relating to preservation and/or access to data on behalf of foreign countries must be explicitly restricted to 'Contracting Parties' or 'Contracting States' to 'the Convention'.

5.1.5 The Absence of a Vulnerability test for Preservation Notices

As highlighted above, Article 16(1) of the Convention allows for preservation of specified computer data in particular situations “where there are grounds to believe that the computer data is particularly vulnerable to loss or modification”. Preservation is therefore only necessary in situations where there is a threat that the data required for an investigation is in danger of being lost or modified. This requirement is completely absent in the Bill. As a consequence, the Bill would authorise the preservation of stored communications at any time and not just in situations where there are grounds to believe that the stored communications in question could be lost or modified. This is an unwarranted extension of the Convention and would extend the scope of preservation notices beyond the Convention’s original intention and would again create a foundation for potential ‘fishing expeditions’.

The Bill should include a vulnerability test for the issuance of a preservation notice, to ensure that such notices are only used where there are reasonable grounds to believe that the data in question might not be available for an investigation in the normal course of events.

5.2 The Security and Integrity of Preserved Data

The Council’s Explanatory Memorandum contends that preservation notices, if implemented within correct procedures and cognisant of the needs of privacy, can provide law enforcement agencies with a flexible mechanism to preserve evidence for ongoing and future criminal investigations.

> 163. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure

> accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data.

This is re-emphasised elsewhere in the Explanatory Memorandum

> 151. … To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. …. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

The Bill, on the other hand, is silent on any obligations on a carrier to store preserved data in a secure manner. While the general security principle in the Privacy Act would apply, this is arguably not specific enough to achieve the protection required by the Convention.

It is essential that a Bill to enable accession to the Cybercrime Convention provide an explicit requirement on carriers to store data subject to a preservation notice in a secure manner as part of the measures to ensure the integrity and confidentiality of the data.

5.3 Lack of context in relation to future Data Retention requirements

The government has for some time been considering introducing a requirement for data retention, at least on telecommunications providers and possibly in other sectors. While there has been no public consultation on this to date, it was picked up by the Senate Environment and Communications Committee in its inquiry last year into Online Privacy. That Committee recommended a cautious approach to such a requirement, with wide consultation (Recommendation 9). We note a report in The Australian newspaper on 26 July 2011 that.the government is still actively considering a data retention regime and draws the obvious link to the preservation regime in the current Bill.

Data retention requirements in other jurisdictions have been highly contentious – not least in the European Union where an existing Directive is currently under review.

We note the following important distinction in the Explanatory Memorandum

> 151. "Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

While this Bill appears not to venture directly into the area of data retention, we believe the Committee, the Parliament and the public need to be given an explanation of the government's current intentions in relation to data retention as important context for the preservation elements of this Bill.

5.4 Grossly Inadequate Privacy Protections

5.4.1 The Necessity of Human Rights Protections Within the Bill

The Convention contained little in this area, because it did not need to – it is obligatory for European nations to have substantive protections in place. That condition that does not hold in Australia.

It is essential that a Bill to enable accession to the Cybercrime Convention include a substantial set of provisions that implement human rights protections that are equivalent to the relevant provisions that provide countervailing rights in CoE countries, and that are the means whereby the CoE Convention represents a balanced instrument.

We refer to the APF's submissions to recent Parliamentary inquiries into proposed general human rights protections[1] for substantive discussion about desirable protections. In the absence of any more general human rights charter, we believe relevant provisions need to be inserted into this Bill.

5.4.2 Meaninglessness of the Privacy Test

The proposed new Division 4B of the TIAA introduces a new privacy consideration for authorising officers, applying both to authorisations under the new foreign assistance provisions (Division 4A) and to authorisations for domestic use under the existing Division 4. While in principle a new privacy test would be welcome, proposed section 180F does not amount to a meaningful test.

An authorising officer has to merely "have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure". This is not in any sense a protection, because it fails to impose an obligation to form a judgement as to whether the extent of interference is justified, and hence it is open to the authorising officer to proceed unfettered.

It is essential that a Bill to enable accession to the Cybercrime Convention specify a meaningful test in every circumstance in which the exercise of any power (including a notice, order or authorisation) is considered. This must be along the lines of 'would a reasonable person conclude that the privacy interests of an individual outweigh the public interest in preserving or disclosing the stored communications of the individual(s) in relation to a domestic or foreign cybercrime investigation?'.

5.4.3 Inappropriate Delegation of the Decision to the Authorising Officer

Determination of the balance between privacy and the public interest by the authorising officer fails the criterion of the power being subject to independent controls.

It is essential that a Bill to enable accession to the Cybercrime Convention specify that determination of the privacy test must be an adjudicative process by an independent body, not a procedural process conducted by the person authorising a disclosure.

5.4.4 Inadequacy of the Oversight Arrangements

The independent oversight that is specified is inadequate.

It is essential that a Bill to enable accession to the Cybercrime Convention create an effective mechanism whereby every circumstance in which the exercise of any power (including a notice, order or authorisation) is subject to effective oversight by a genuinely independent body that has substantial powers and resources to investigate and enforce, and transparency to the public.

[1] National Human Rights Consultation, 2009; Human Rights (Parliamentary Scrutiny) Bill 2010, NSW Draft Bill of Rights 2011

5.4.5 Absence of Standards-Assurance Regarding the Identification of Individuals

One of the privacy benefits of the proposed preservation notices *may be* that an issuing agency can only apply for a notice on one individual at a time (subject to confirmation – see 5.1.2 above) . However there will remain a serious risk that the wrong individuals may be inadvertently targeted. Any person to be subject of a preservation notice needs to be reliably identified, including in situations where considerable ambiguity and uncertainty exist, such as multi-person households and people with similar names.

It is essential that a Bill to enable accession to the Cybercrime Convention create specify a process and standards relating to the reliable identification of the targeted individual.

5.4.6 Failure to Adequately Limit Secondary Uses

We are concerned about the limits of secondary use restrictions in relation to foreign disclosures under the proposed s180E of the TIAA. Section 180E intends to restrict when information or documents disclosed to a foreign country can be disclosed to a foreign country under s180B. The Attorney-General is able to impose conditions to be complied with prior to the disclosure of information. These include restrictions on the use of information disclosed only for the purpose for which the foreign country requested it, stipulations regarding the destruction of the disclosed data and any other condition that may be required.

However, conditions can only imposed on disclosures under s180B as those under s180A and s180C would be conducted on an agency to agency basis and would therefore be made without the approval or oversight of the Attorney-General.

Any information disclosed from Australia to a foreign country must have specific restrictions that prohibit the secondary use of disclosed information. It should be irrelevant whether the information disclosure is conducted through an agency to agency transfer or one governed by restrictions made by the Attorney-General.

Furthermore, it is unclear what oversight mechanisms exist in relation to potential secondary uses by foreign countries. Other than the instigation of limited restrictions at the point of disclosure, it is unclear how the Australian Government would be able to ensure that these restrictions are being adhered to. Again, this re-emphasises the need, which we have already stated above, for the meaning of ‘foreign countries’ in this Bill to be restricted to those States that are parties to the Convention.

It is essential that a Bill to enable accession to the Cybercrime Convention:

- **impose strict limitations on the purposes for which data may be preserved, collected, used and disclosed**
- **expressly prohibit all secondary uses of all such data**
- **include no loopholes of the kind inserted in the present Bill**
- **ensure that those limitations are imposed on any other person that may come into possession of the data**

5.4.7 Inadequate Protection of Data Sent Overseas

In relation to foreign disclosure, there is an inadequate oversight mechanism relating to the use of disclosed information, no way to take action in relation to an unauthorised secondary use, nor any obligation not to disclose in the event that reasonable grounds exist for believing that the foreign agency will not comply with the conditions.

The gravity of this problem is all the greater because of the serious flaw identified in 1.4 above, whereby the Bill permits disclosure to countries that have not acceded to the Convention and hence may not have appropriate protections in place.

It is essential that a Bill to enable accession to the Cybercrime Convention:

- **ensure that all of the limitations required under s.3.6 above are imposed on any other person that may come into possession of the data**
- **create an obligation not to disclose in the event that reasonable grounds exist for believing that the recipient may not comply with the conditions**

5.5 Inadequate Implementation of the 'Dual Criminality' Principle

5.5.1 Failure to Defend National Sovereignty

It is fundamental to national sovereignty that a person's behaviour must not be subject to the powers of Australian national security and law enforcement agencies unless that behaviour is criminal in this country.

Powers must not be granted in respect of behaviour that would not be a crime if performed in Australia. An Australian citizen must be protected against abuse of their communications, their data, their freedom within Australia, and their freedom against extradition actions. The Bill, as currently constructed does not explicitly recognise this principle. The proposed s5EA, which would be inserted in to the TIAA defines a serious foreign contravention as:

> A contravention of a law of a foreign country that is punishable by a maximum penalty of:
> (a) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
> (b) a fine of an amount that is at least equivalent to 900 penalty units.

The Bill's Explanatory Memorandum indicates that clause (b) relates to s4AA of the Crimes Act 1914. The construct of 'serious foreign contravention' is used as the basis for a foreign preservation notices and further mutual assistance actions. The Bill's Explanatory Memorandum states clearly that the intention is for a foreign stored communications warrant to have a similar domestic counterpart offence:

> A similar penalty threshold will ensure that stored communications warrants for foreign offences will only be able to be issued where a warrant for a domestic investigation would also be able to be issued.

This point is re-emphasised in the reporting requirements for mutual assistance applications in relation to foreign stored communications warrants under the proposed s162(1)(d) of the TIAA

> (c) the relevant statistics about mutual assistance applications that the agency made during that year; and
> (d) for each offence (the foreign offence) against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made by the agency during the year—the offence (if any), under a law of the Commonwealth, or of a State or a Territory, that is of the same nature as, or a substantially similar nature to, the foreign offence.

There is undoubtedly an intention to respect the principle of dual criminality in the Bill. However, as constructed s5EA allows for the situation in which a serious foreign contravention can be an infringement of a foreign law that may or may not have a corresponding Australian equivalent due to the use of 'or' between sub-clause (a) and (b). The use of 'or' rather than 'and' does not make Australian equivalence a condition of a 'serious foreign contravention' because a contravention of a foreign law will alone be suffice.

We suggest therefore that the wording of s5EA be changed to explicitly recognise a dual criminality principle as below:

> A contravention of a law of a foreign country that is punishable by a maximum penalty of:
> (a) imprisonment for 3 years or more, imprisonment for life or the death penalty; and
> (b) there is an equivalent or substantially similar law of the Commonwealth, or of a State or a Territory.

It is essential that a Bill to enable accession to the Cybercrime Convention not grant powers in respect of behaviour that would not be a crime if performed in Australia. Australian citizens must be protected against abuse of their communications, their data and their freedoms in relation to conduct that is lawful within Australia.

5.5.2 'Speech Crimes'

In particular, the Bill potentially creates situations in which Australian government agencies could inadvertently assist foreign governments in the repression of political speech in ways repugnant to Australian law.

This arises in part because the Bill refers to 'foreign countries' and not parties to the Convention, although it could also arise in respect of countries that accede, but whose laws and practices are not compliant with the Convention's terms.

By way of relevant and important potential example, the Government of the PRC could request the preservation, collection and disclosure to it of stored computer data in relation to 'dissidents' in Australia who have committed a 'serious Chinese contravention', e.g. political criticism of the State or even the Party that could give rise to a prison sentence above 3 years. This would of course not even be a crime in Australia, let alone a crime that reaches the relevant threshold. It is completely inappropriate for Chinese dissidents resident in Australia to be dependent on the Attorney-General exercising a discretion not to authorise preservation, collection and/or disclosure in such circumstances.

It is essential that a Bill to enable accession to the Cybercrime Convention neither grant powers nor create obligations to foreign governments that have the effect of chilling the political speech of persons resident in Australia.

6. Excessive Confidentiality

Schedule 4 introduces confidentiality provisions which make it an offence to disclose information about authorisations under Chapter 4 of the TIAA. The only exceptions are for the interests of the accessing agencies and for missing persons cases.

While we accept the need to keep the existence, and content, of authorisations, secret *where disclosure would prejudice the purpose of the authorization, and related investigations* (our emphasis), the blanket confidentiality provisions in the Bill are excessive and repugnant. As APF has consistently argued in relation to interception warrants, there is no justification for keeping information about law enforcement and national security access to telecommunications data secret, at least from the data subjects, once any prejudice no longer exists.

We also seek assurances that confidentiality provisions will not apply, at least in a blanket way, to the existence and content of preservation notices. The same qualifications should apply to these – i.e. that they can and should be kept secret from the subjects (customers of the relevant services) only where, and for as long as, this is necessary so as not to prejudice investigations.

Information about access under the TIAA should at least be accessible by relevant data subjects under the FOI Act, and consideration should also be given to requiring law enforcement and

national security agencies to pro-actively inform data subjects that their communications have been accessed, once such knowledge would no longer prejudice investigations.

The prevailing mindset of law enforcement and national security agencies is to keep their activities as secret as possible, and fails to acknowledge either the individual rights or accountability arguments for greater transparency.

It is essential that a Bill to enable accession to the Cybercrime Convention strictly limit suppression of information about authorisations firstly to circumstances in which disclosure would prejudice the purpose of the authorisation, and related investigations, and secondly, even then, only for as long as this is necessary so as not to prejudice investigations.

It is highly desirable that a Bill to enable accession to the Cybercrime Convention oblige law enforcement and national security agencies to pro-actively inform data subjects that their communications have been accessed, once such knowledge would no longer prejudice investigations.

7. The Likelihood of Additional Highly Deleterious Features and Effects

Because of the obstructions placed in the way of careful consideration and analysis of the Bill, as noted in 4 above, it is impossible for interested parties to conduct and deliver an assessment that can be assured to be comprehensive. The serious deficiencies identified in the previous section are therefore unlikely to be the only ones present in the Bill.

For example, the APF and others are particularly concerned that the Government may have in mind to use measures in this Bill as a means of achieving Internet censorship by adopting the pretence that it is authorised as a form of cooperation with overseas law enforcement agencies.

Similarly, there must be real fears that accession to the Cybercrime Convention, and the provisions of this legislation, will lead to unacceptable intrusion into internet use in order to enforce intellectual property rights claims by (mostly US) businesses. A broad coalition of international Civil Society NGOs recently declined to endorse OECD Internet Policy Principles on the basis that the proposed principles favoured business IP rights over individuals' rights and freedoms (see http://csisac.org/).

8. Conclusions

In summary:

- the Bill has been placed before the Parliament in a manner that obstructs understanding of its meaning and analysis of its impacts
- the Bill seeks to impose all of the intrusive elements of the Convention without allowing for the Convention's presumption that strong human rights protections are in place. As a result, its provisions would create grossly unbalanced and excessive legislative powers
- despite its claimed purpose, the Bill goes well beyond what is necessary in order to accede to the Convention, and the extensions are highly privacy-abusive
- despite the barriers to understanding, the APF has identified 14 serious features that should under no circumstances be passed into law
- the Bill very probably contains further excessive features that cannot be readily detected because of both the inherent and contrived complexities in the material provided
- the APF submits that the Committee must find that, in its present form, the Bill is completely unacceptable, and incapable of amendment into an acceptable form

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/