Parliament of Australia
Department of Parliamentary Services

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

BILLS DIGEST NO. 31, 2011–12 18 August 2011

# Cybercrime Legislation Amendment Bill 2011

Mary Anne Neilsen
Law and Bills Digest Section

## Contents

Purpose ..... 4
Background ..... 4
Cybercrime and the Council of Europe Convention on Cybercrime ..... 4
Outline of the Convention ..... 6
Committee consideration ..... 7
House of Representatives Standing Committee on Communications—2010 Report of the Inquiry into Cybercrime ..... 7
Parliamentary Joint Standing Committee on Treaties—Report on the Europe Convention on Cybercrime ..... 8
Joint Select Committee on Cyber-Safety inquiry ..... 8
Senate Scrutiny of Bills Committee ..... 8
Position of major interest groups ..... 9
Law Council of Australia ..... 9
Electronic Frontiers Australia ..... 9
State Governments ..... 10
Queensland Council for Civil Liberties ..... 10
Commonwealth Ombudsman ..... 10
Australian Privacy Foundation ..... 11
Telstra ..... 11
Cyberspace Law and Policy Centre ..... 11
Financial implications ..... 11

ISSN 1328-8091

Main issues ..... 12
Dual criminality and thresholds for the issuing of a warrant ..... 12
Protection of privacy ..... 14
Key provisions ..... 17
Schedule 1 – Preservation regime for stored communications ..... 17
Overview ..... 17
Telecommunications Act 1997 ..... 17
Telecommunications (Interception and Access) Act 1979 ..... 18
Preserving stored communications ..... 18
Domestic preservation notices ..... 18
Foreign preservation notices ..... 20
Miscellaneous provisions relating to both domestic and foreign preservations notices ..... 21
Comment on Schedule 1 ..... 22
Schedule 2 – Amendments relating to mutual assistance ..... 24
Overview ..... 24
Part 1—Stored communications warrants ..... 25
Mutual Assistance in Criminal Matters Act 1987 ..... 25
*Telecommunications (Interception and Access) Act 1979* ..... 25
Comment on Part 1—Amendments relating to stored communications warrants ..... 27
Part 2 – Amendments relating to telecommunications data ..... 28
Mutual Assistance in Criminal Matters Act 1987 ..... 28
*Telecommunications Act 1997* ..... 29
Telecommunications (Interception and Access) Act 1979 ..... 29
Comment on Part 2—Amendments relating to telecommunications data ..... 31
Schedule 3— Criminal Code Amendments ..... 32
Criminal Code Act 1995 ..... 32
Comment on Schedule 3 and the Criminal Code amendments ..... 33
Schedule 4—Telecommunications data confidentiality ..... 36
Overview ..... 36
Telecommunications (Interception and Access) Act 1979 ..... 36

Comment on Schedule 4 ..... 37
Concluding comments ..... 37

# Cybercrime Legislation Amendment Bill 2011

**Date introduced:** 22 June 2011

**House:** House of Representatives

**Portfolio:** Attorney-General

**Commencement:** Schedules 1, 2, 4 and 5 commence the 28th day after Royal Assent. Schedule 3 commences the later of the day of Royal Assent and the day the Council of Europe Convention on Cybercrime comes into force for Australia. However the provisions in Schedule 3 do not commence at all unless the Convention comes into force within 6 months of Royal Assent.

**Links:** The links to the the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill's home page, or through http://www.aph.gov.au/bills/. When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the ComLaw website at http://www.comlaw.gov.au/.

## Purpose

The Cybercrime Legislation Amendment Bill 2011 (the Bill) amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Criminal Code Act 1995* (the Criminal Code Act), the *Mutual Assistance in Criminal Matters Act 1987* (the MA Act) and the *Telecommunications Act 1997* (the Telecommunications Act) to ensure that Australian legislation is compliant with the Council of Europe Convention on Cybercrime requirements in order to facilitate Australia's accession to the Convention.

## Background

### Cybercrime and the Council of Europe Convention on Cybercrime

Cybercrime has been described as including:

> criminal activity involving use of computers or computer networks, such as in unlawfully accessing computer data or interfering with computer systems, or where computer use is integral to the offence, such as for the distribution of child pornography via the Internet.[1]

It is generally acknowledged that cybercrime is a growing threat to consumers, commensurate with the value and significance of electronic communications as the most efficient, dynamic and prolific global mechanism for social, professional and business communications.[2]

The Council of Europe Convention on Cybercrime (the Convention), which opened for signature in Budapest on 23 November 2001, entered into force on 1 July 2004.[3] The Convention is the first international treaty in this area, its main objective being to:

> …develop a common criminal policy to combat cyber crime, in particular by adopting appropriate legislation and international co-operation.

To date, 31 countries, (including the United States) are party to the Convention and a further 16 others have signed the Convention including non-members Canada, Japan and South Africa.[4] On 30 April 2010, the Australian Government announced its intention to accede to the Convention, the Attorney-General and the Minister for Foreign Affairs stating:

> The Convention is the only binding international treaty on cybercrime. It serves as both a guide for nations developing comprehensive national legislation on cybercrime and as a framework for international co-operation between signatory countries.
>
> Cybercrime poses a significant challenge for our law enforcement and criminal justice system. The Internet makes it easy for criminals to operate from abroad, especially from those countries where regulations and enforcement arrangements are weak.
>
> It is critical that laws designed to combat cybercrime are harmonised, or at least compatible to allow for co-operation internationally.[5]

---

1. Parliamentary Joint Standing Committee on Treaties, *Report 116 Treaties tabled on 11 May 2011,* Chapter 11, Canberra, 2011, paragraph 11.2, viewed 18 July 2011, http://www.aph.gov.au/house/committee/jsct/1march2011/report.htm
2. Ibid, paragraph 11.7. For further background on the problems of tackling cyber crime the reader is referred to: House of Representatives Standing Committee on Communications, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, *the Report of the Inquiry into Cyber Crime, Commonwealth of Australia, June 2010,* viewed 16 August 2011, http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf
3. Council of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, viewed 15 August 2011, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
4. Council of Europe, *Convention on Cybercrime,* CETS No.: 185, viewed 15 August 2011, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG
5. R McClelland, (Attorney-General) and K Rudd (Minister for Foreign Affairs), *Accession to the Council of Europe Convention on Cybercrime*, media release, 11 May 2011, viewed 15 August 2011, http://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/757574/upload_binary/757574.pdf;fileType=application/pdf#search=%22Accession%20to%20the%20Council%20of%20Europe%20Convention%20on%20Cybercrime%22

On 17 February 2011, the Attorney-General's Department (AGD) released a public discussion paper in relation to Australia's proposed accession to the Convention.[6] This was followed on 1 March with the tabling of the national interest analysis by the Minister for Foreign Affairs and referral of the question of ratification to the Parliamentary Joint Standing Committee on Treaties.

## Outline of the Convention

The Convention promotes a coordinated approach to cybercrime by requiring countries to criminalise four types of offences, including:

- offences against the confidentiality, integrity and availability of computer data and systems, including illegal access to computer systems, illegal interception, data interference, systems interference and the misuse of devices
- computer-related offences, including forgery and fraud
- content-related offences, including child pornography and
- offences related to the infringement of copyright and other related rights.

It also establishes procedures to make investigations more efficient and provides systems to facilitate international co-operation, including:

- helping authorities from one country to collect data in another country
- empowering authorities to request the disclosure of specific computer data
- allowing authorities to collect or record traffic data in real-time
- establishing a 24/7 network to provide immediate help to investigators and
- facilitating extradition and the exchange of information.[7]

The Convention also contains provisions explicitly requiring that enforcement powers and procedures established under the Convention are to be conducted with respect for fundamental human rights, such as for free expression, the right to access information of all kinds and the right for privacy and protection of personal data.[8]

---

6. Attorney-General's Department, *Public consultation document: Outline of the Articles of the Council of Europe Convention on Cybercrime and Australia's compliance*, 2011, viewed 15 August 2011, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Approved+-+TSLB+-+LSD+-+FINAL+APPROVED+public+consultation+outline+of+articles+-+cybercrime+convention+-+18+February+2011.pdf/$file/Approved+-+TSLB+-+LSD+-+FINAL+APPROVED+public+consultation+outline+of+articles+-+cybercrime+convention+-+18+February+2011.pdf
7. This summary relies on: R McClelland, (Attorney-General) and B O'Connor (Minister for Home Affairs and Justice), *Public consultation on International Cybercrime Convention*, media release, 18 February 2011, http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2011_FirstQuarter_18February2011-PublicconsultationoninternationalCybercrimeConvention
8. Parliamentary Joint Standing Committee on Treaties, op. cit., paragraph 11.5.

The Government has indicated that in the main Australia's laws comply with the Convention, noting also that Australia has specific laws targeting cyber crime.[9]

Further information on specific articles of the Convention that relate to the Bill is set out in the Main issues and Key provisions sections of the Bills Digest. For a fuller outline of the Convention the reader is referred to the AGD public consultation document on the Convention referred to above.

## Committee consideration

Several parliamentary committees have examined the question of Australia's accession to the Convention and the related Bill.

### House of Representatives Standing Committee on Communications—2010 Report of the Inquiry into Cybercrime

In June 2010, the House of Representatives Standing Committee on Communications tabled a report on cybercrime called *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, *the Report of the Inquiry into Cyber Crime* (the Report).

The Report includes consideration of the Convention with one of the Committee's recommendations being that the Federal Attorney-General, in consultation with state and territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.[10]

The Government, in its response to the Report accepted this recommendation, noting that Australia intends to accede to the Convention and that 'Australia is currently in a good position to comply with the majority of obligations under the Convention. The Government is working on the final legislative amendments required for Australia to formally accede.'[11]

9. R McClelland, (Attorney-General) and K Rudd (Minister for Foreign Affairs) op. cit.
10. Ibid., Recommendation 9.
11. R McClelland (Attorney-General) and S Conroy (Minister for Broadband, Communications and the Digital Economy), *Government Response: Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime,* House of Representatives, Standing Committee on Communications, Report on the Inquiry into Cyber Crime*,* 25 November 2010, viewed 16 August 2011, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(689F2CCBD6DC263C912FB74B15BE8285)~Government+response+-+Report+on+the+inquiry+into+Cyber+crime+-+Hackers+Fraudsters+and+Botnets++Tackling+the+Problem+of+Cyber+Crime+PDF.pdf/$file/Government+response+-+Report+on+the+inquiry+into+Cyber+crime+-+Hackers+Fraudsters+and+Botnets++Tackling+the+Problem+of+Cyber+Crime+PDF.pdf

## Parliamentary Joint Standing Committee on Treaties—Report on the Europe Convention on Cybercrime

As noted above, Australia's ratification of the Convention was considered by the Parliamentary Joint Standing Committee on Treaties following referral on 1 March 2011 (JSCOT or JSCOT inquiry). In its Report tabled on 11 May 2011 JSCOT recommended ratification, although it expressed some concerns:

> [...] the Committee holds concerns about the lack of transparency in the review process for this important treaty, in particular, the lack of timely advice to the Committee and the lack of public exposure and certainty about necessary amendments to support Convention obligations.

With reference to this, the Committee supports binding treaty action being taken but also recommends the Attorney-General's Department should report to the Committee on the content and purpose of any proposed amendments.[12]

## Joint Select Committee on Cyber-Safety inquiry

Following introduction of the Bill into Parliament, on 23 June 2011, the House of Representatives Selection Committee requested that the Joint Select Committee on Cyber-Safety inquire into and report on the Bill (the JSC inquiry).[13]

Submissions to the JSC Cyber-Safety inquiry are referred to in other sections of the Bills Digest.

## Senate Scrutiny of Bills Committee

The Senate Scrutiny of Bills Committee has also examined the Bill and suggested that some of the provisions in Schedules 1 and 2 may raise privacy concerns.[14] However while noting that there may be concerns about the disclosure of personal information, the Committee also acknowledged that the Bill contains a number of important protections and accountability mechanisms. The Committee therefore has left to the Senate as a whole, the question of whether the Bill strikes an appropriate balance of the right to privacy and the policy objectives associated with the implementation of the Convention.[15]

12. Parliamentary Joint Standing Committee on Treaties, op. cit., paragraphs 11.63–11.64.
13. Details of the inquiry are at: http://www.aph.gov.au/house/committee/jscc/cybercrime_bill/index.htm
14. Senate Standing Committee for the Scrutiny of Bills, *Alert Digest*, no. 7, 2011, viewed 15 August 2011, http://www.aph.gov.au/Senate/committee/scrutiny/alerts/2011/d07.pdf
15. Ibid., p. 4.

## Position of major interest groups

To date, there are 22 submissions to the JSC inquiry available on the Committee website. They present a diverse range of views—a few submissions support the Bill without reservation and a few reject in principle Australia's ratification of the Convention. Many other submissions, while supportive of ratification of the Convention, expressed concerns about specific provisions in the Bill, particularly in relation to issues of individual rights and privacy protections and on the capacity of the states and territories to retain and implement relevant enforcement powers within their jurisdictions. This section is selective and provides only a small selection from those submissions. Further comment can be found in the Main issues and Key provisions sections of the Bills Digest.

### Law Council of Australia

The Law Council has a number of concerns particularly about the amendments proposed in Schedule 2 of the Bill (provisions relating to mutual assistance), and submits that these require further consideration and revision before they are enacted.[16]

While not objecting to the aims of the amendments in principle, the Law Council expressed concern about a lack of rigour in the proposed threshold tests, reporting obligations and privacy safeguards which would apply to authorisations to access and disclose information about stored communications and telecommunications for the purposes of a foreign investigation.

The Law Council also noted that the form of the relevant amendments is in no way dictated by the Convention and that the Government is therefore not constrained by the Convention in responding to and addressing the concerns raised by the Law Council.[17]

More specific concerns of the Law Council are considered in the Main provisions and Key issues sections of the Bills Digest.

### Electronic Frontiers Australia

Electronic Frontiers Australia (EFA)[18], in its submission, states that it is on record as having argued against many of the proposals in the Convention since the drafting stage and still feels that the Convention is very problematic. In its opinion, the Bill has confirmed this view and EFA remains concerned about the combination of a lack of mutual criminality proceedings and feels that there needs to be strong protection against foreign requests for assistance with regard to offences with

16. Law Council of Australia, Submission to the Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011, p. 3.
17. Ibid.
18. EFA, established in 1994, is a non-profit national organisation representing Internet users concerned with online rights and freedoms.

political elements. While appreciating that the assent of the Attorney General is required with regard to some requests, EFA believes that issues remain.

EFA's major concerns, however, are with Schedule 3 and the strong expansion of applicability of the computer offences under the Criminal Code Act:

> The minimum amendments have been made to allow the necessary coverage required by the Convention, but we feel this expands the applicability of the offences far too widely.[19]

### State Governments

The Victorian and Western Australian State Governments raise specific concerns with Schedule 3 and the expansion of applicability of the offences under the Criminal Code Act. They argue that the provisions in that Schedule could be problematic as a result of the High Court decision in *Dickson v R*[20] and for this reason the Bill should be deferred.[21]

### Queensland Council for Civil Liberties

The Queensland Council for Civil Liberties argues the Bill should be rejected and their submission is critical of both the Convention and the Bill. Amongst other things they note a lack of dual criminal provisions, a lack of transparency and conclude by arguing:

> 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.[22]

### Commonwealth Ombudsman

The Commonwealth Ombudsman's submission focuses on the preservation amendments in Schedule 1. While acknowledging the purpose and benefits of the amendments, the Commonwealth Ombudsman has several concerns with the practical operation of the preservation notices scheme. The submission also recommends a broader scope for the Ombudsman's oversight function in relation to the preservation scheme. He suggests that the powers of the Ombudsman to inspect and

19. Electronic Frontiers Australia, Submission to the Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011.
20. (2010) 241 CLR 491, [2010] HCA 30.
21. R Clark, (Attorney-General, Victoria) *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Select Committee on Cyber-Safety, August 2011; C Barnett (Premier, WA), *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Select Committee on Cyber-Safety, August 2011. For a discussion of Dickson see pp. 34-35 of the Bills Digest. In brief the High Court held a Victorian conspiracy provision to be inconsistent with the Criminal Code's provision and therefore invalid to the extent of that inconsistency.
22. Queensland Council for Civil Liberties *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Select Committee on Cyber-Safety, August 2011.

audit compliance with the preservation regime require clarification to ensure he/she can check compliance with the TIA Act rather than having a mere record keeping role.[23]

### Australian Privacy Foundation

The Australian Privacy Foundation states that it is sympathetic to the stated objective of the Bill and that it considers that mutual assistance and cooperation is desirable to combat the problems of some types of cybercrime, including aspects of cybercrime that go directly to issues of privacy.

However, it also argues that the Convention is flawed and more significantly, that the Bill goes well beyond what is required for mere accession to the Convention and that the extensions are 'highly privacy-abusive'.[24]

### Telstra

Telstra is generally supportive of the Bill and believes the amendments will assist in streamlining procedures between carriers and law enforcement agencies in the preservation of stored communications. Telstra's main concern is with the timeframe for implementation which they argue will be problematic for the various carriers involved in the new preservation regime.[25]

### Cyberspace Law and Policy Centre

The Cyberspace Law and Policy Centre wholly supports ratification of the Convention and believes that the measures in the Convention are fundamental to combating cybercrime. However CLPC is also concerned that some of the proposed amendments go beyond the commitments found in the Convention. While some of this expansion is necessary to better fight cybercrime CLPC also argues that better safeguards are needed to prevent the abusive use of such powers.[26]

## Financial implications

The Explanatory Memorandum states that the Bill will have no financial impact.[27]

23. Commonwealth Ombudsman, *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Select Committee on Cyber-Safety, August 2011, p. 4.
24. Australian Privacy Foundation, *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Standing Committee on Cyber-Safety, August 2011.
25. Telstra, *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Standing Committee on Cyber-Safety, August 2011.
26. Cyberspace Law and Policy Centre, *Cybercrime Legislation Amendment Bill 2011*, Submission to the Joint Standing Committee on Cyber-Safety, August 2011, paragraph 1.0.
27. Explanatory Memorandum, *Cybercrime Legislation Amendment Bill 2011*, p. 2.

# Main issues

This section of the Bills Digest focuses on only two of the issues raised in submissions to the JSC inquiry. The reader is also referred to the Key provisions section of the Bills Digest for further analysis of other issues.

## Dual criminality and thresholds for the issuing of a warrant

Several submissions argue that the Bill does not explicitly recognise the dual criminality principle. Under this principle it is argued that powers must not be granted 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.

Questions of dual criminality regarding the Bill have arisen in relation to the new definition of a 'serious foreign contravention'. The Bill proposes to insert a new definition into the TIA Act (**proposed section 5EA, item 7, Schedule 2**), which defines a 'serious foreign contravention' as a contravention of a foreign law which has a penalty of three years imprisonment or more, imprisonment for life or the death penalty, or a fine for an amount of at least 900 penalty units. This definition of 'serious foreign contravention' is central to many of the provisions of the Bill and it is used as a threshold test for the grant of various powers. For example, when determining whether to issue a stored communications warrant for the investigation of a foreign offence, the authorised police office must consider if the investigation the foreign country is investigating is a serious foreign contravention.

The Explanatory Memorandum states that the rationale for this definition is to provide consistency with the penalty threshold for stored communications warrants for domestic offences, which is a period of at least three years imprisonment or 900 penalty units.[28]

However, in the view of many submitters to the JSC inquiry, it is likely that foreign countries may, in some instances, have higher penalties for similar offences and that effectively lowers the threshold for the issue of the stored communications warrant for foreign offences. This, they argue flouts the principle of dual criminality.

In relation to this issue, the Cyberspace Law and Policy Centre notes that Australia has a more limited set of cybercrimes than exist in many other countries. Their submission notes:

> A good example is that sedition is no longer a criminal offence in Australia, yet it remains a criminal offence in many other countries, including some countries in the region. That is a core part of our test of whether or not the bill is acceptable: whether or not there is a clear and unambiguous requirement for dual criminality. The convention allows countries to make

28. Ibid., p. 20

> reservations related to dual criminality requirements, so it is already anticipated that countries would do that.[29]

The Law Council also argues that it should not be possible under the MA Act and the TIA Act for foreign law enforcement agencies to obtain, coercively or by compulsion, material that they would not be able to access if they were a domestic law enforcement agency investigating the same conduct. [30] The Law Council submits that the relevant provisions should be amended to require that offence under investigation would attract the requisite threshold penalty had it been committed in Australia.[31]

In response to these concerns, an officer from AGD at the JSC inquiry hearings stated:

> In relation to access to stored communications and access to prospective telecommunications data, the foreign country can only access those types of data under a formal mutual assistance request, and all the safeguards set out in the Mutual Assistance Act that currently apply will apply to these new law enforcement powers for foreign purposes. So all of the grounds for refusal set out in section 8, including dual criminality, will apply to any request by a foreign country to access stored communications and prospective telecommunications data.[32]

While AGD officers alluded to the significance of section 8 of the MA Act at the JSC inquiry hearings, the Bill, the Second Reading Speech or Explanatory Memorandum do not specifically refer to the protections set out in that provision. Given the concerns expressed by so many submitters, it would seem that the understanding of the Bill could be improved by inserting in relevant provisions a reference to the protections in section 8 of the MA Act as being part of the threshold test for the grant of the new powers.

This is also a suggestion of the Law Council in their analysis of **proposed sections 180B and 180C** of the TIA Act. These provisions provide that disclosures may be made to a foreign law enforcement agency on the conditions that it:

- is reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and
- appropriate in all the circumstances.

In relation to the term 'appropriate in all the circumstances' the Explanatory Memorandum provides that this is:

---

29. D Vaile (Executive Director, CLPC), Joint Select Committee on Cyber-Safety, *Committee Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 12.
30. Law Council of Australia, op. cit., p. 5.
31. Ibid.
32. A Kiley (Senior Legal Officer, Telecommunications and Surveillance Law Branch, AGD), Joint Select Committee on Cyber-Safety, *Committee Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 29.

> [...] intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.[33]

The Law Council suggests this explanation unhelpful and that the use of the term 'appropriate in all the circumstances' is far too ambiguous to act as an effective safeguard and provides no guidance to the relevant officer about the types of matters that the legislature intends that he or she will consider before authorising the disclosure.[34] The Law Council suggests that the provision at least be amended to provide that:

> Without limiting subsection 180(5)(b) and 180C(2), in determining whether a disclosure is appropriate in all the circumstances, the authorising officer must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request as listed in section 8 of the Mutual Assistance Act.[35]

This, the Law Council argues would ensure that the authorising officer is at least required to consider matters such as whether the disclosure relates to:

- an investigation into a purely political offence
- an investigation into conduct that doesn't even constitute an offence in Australia
- an investigation which is designed to punish or otherwise cause prejudice to a person on account of his or her race, sex, religion, nationality or political opinions, or
- an investigation which might result in the imposition of the death penalty.[36]

## Protection of privacy

A common theme that comes through submissions to the JSC inquiry is the issue of privacy protection and in particular a shared concern that **new section 180F** in the TIA Act will not be strong enough to protect personal privacy.

Currently under **subsection 180(5)** of the TIA Act before authorising the disclosure of prospective telecommunications data in the context of a domestic investigation, an authorised officer must first 'have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.' There is no like requirement in the TIA Act to consider privacy impacts when authorising the disclosure of historical telecommunications data.

The Bill proposes to repeal **subsection 180(5)** (**item 40**) and replace it with a **new section 180F** (**item 41, Schedule 2**). This new section would impose a uniform requirement on an authorising officer to '*have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure or use'* before issuing an authorisation, regardless of whether the authorisation

33. Explanatory Memorandum, p. 37.
34. Law Council of Australia, op. cit., p. 8.
35. Ibid.
36. Ibid., p. 9.

relates to prospective or historical telecommunications data and is issued in the context of a domestic or foreign investigation.

The Explanatory Memorandum states that for the purposes of the Bill, privacy is intended to be interpreted more broadly than is considered by the *Privacy Act 1988*:

> The Bill's intent is for wider considerations to be made prior to making an authorisation, including the amount of information that making the authorisation will give the agency, the relevance of the accessed information to the investigation in question, as well as how third parties' privacy may be impacted by accessing this information.[37]

The Law Council's submission on this provision is well argued and appears reasonable. While acknowledging that the insertion of section 180F, a provision of broader application than existing subsection 180(5), is a move in the right direction, the Law Council still has concerns about the formulation of this section and its ability to offer an effective privacy safeguard. The submission goes on:

> The Law Council questions the value of a legislative provision which merely requires an authorising officer to "have regard to" privacy impacts.
>
> A legislative direction of this kind may be useful in the context of administrative decision-making, where the decision maker has the benefit of competing submissions and where the exercise of his or her discretion is subject to review. However, in a law enforcement context a more prescriptive test is required.
>
> All authorisations to disclose telecommunications data will necessarily impact upon or interfere with a person's privacy. In the circumstances, the Law Council questions where proposed section 180F leaves the authorised officer, except perhaps with an obligation to tick a box on a template form to indicate that he or she has considered the privacy ramifications of his or her authorisation.
>
> [...]
>
> The Law Council submits that the proposed section should be amended so that it is expressed in terms of a clear test to be applied by the authorised officer. The Law Council suggests, for example, that the subsection could provide as follows:
>
> "Before making an authorisation, an authorised officer must be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons."[38]

At the JSC inquiry hearings, and in response to a suggestion that **proposed section 180F** may be 'vague and meaningless' an AGD officer defended the provision arguing:

37. Explanatory Memorandum, p. 43.
38. Law Council of Australia, op. cit., pp. 10–11.

> It is the language that is already used in the legislation in relation to access to prospective data, which is information that is non-content information that is obtained on a prospective basis. We believe it is an appropriate proportionality test. The act (sic), in effect, prohibits access to any communications, and then access has to be on the basis of lawful authority. That now, including this in this case, will mean that every type of access done with that has a privacy question in it. We consider that it is consistent with what is currently used in other parts of the act, and from our understanding—and certainly the AFP might have something to say on this—they do consider the privacy versus the law enforcement need. There is a balance test done on every occasion, but that is obviously done internally. The language is strictly because it is the language that is consistent with what is already used, rather than bring in too many new definitions.[39]

There are also other provisions in the Bill that deal with the protection of information including **proposed section 142A** of the TIA Act (**item 20, Schedule 2**) and proposed **section 180E** (**item 41, Schedule 2**). **Proposed section 142A** provides that information obtained under a warrant as a result of a mutual assistance application may only be communicated to a foreign country under certain conditions. These conditions are that the information will only be used for the purposes it was requested, that the material will be destroyed when no longer required for those purposes, and any other conditions determined by the Attorney-General. **Proposed section 180E** imposes similar conditions in relation to the disclosure of telecommunications data to a foreign country.

While supporting the imposition of conditions on the transfer of data and information, the Law Council and others query how, in the absence of an undertaking, these conditions could be communicated, imposed, accepted and enforced. The Law Council queries who, in the receiving country, might be regarded as sufficiently authorised to agree to such conditions and then to oversee their observance.[40]

The Law Council's recommendation is that subsection 8(2) of the MA Act be amended to insert an additional discretionary ground for refusing a mutual assistance request, which would encourage the Attorney-General to decline a request for refusing a mutual assistance request, where the requesting country's arrangements for handling personal information do not offer privacy protections substantially similar to those applying in Australia.[41]

39. C Smith (Assistant Secretary, Telecommunications and Surveillance Law Branch, AGD), Joint Select Committee on Cyber-Safety, *Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 33.
40. Law Council of Australia, op. cit., p. 7.
41. Ibid.

# Key provisions

## Schedule 1 – Preservation regime for stored communications

### Overview

The stored communications provisions of the TIA Act are set out in Chapter 3 of the TIA Act and apply to communications such as emails, SMS and voice mail messages that are stored on a carrier's equipment (that is communications that either have not commenced, or have completed passing over a telecommunications system).[42] The chapter establishes the general prohibition on accessing stored communications, the warrant regime exception for enforcement agencies and the accountability and oversight mechanisms.

Schedule 1 of the Bill amends the TIA Act and the Telecommunications Act to oblige carriers[43] to preserve targeted stored communications when requested by certain domestic agencies or when requested by Australian Federal Police (AFP) on behalf of certain foreign countries. The Explanatory Memorandum notes that this Schedule implements requirements of the Convention, particularly Articles 16 and 29. Article 16 requires Parties to establish powers for domestic agencies to obtain the preservation of stored computer data stored communications, including traffic data for up to 90 days, particularly where there are grounds to believe that the data is vulnerable to loss or modification. Article 29 requires Parties to establish powers enabling a domestic agency to be able to obtain the preservation of stored computer data (including traffic data) at the request of other parties to the Convention.[44]

### Telecommunications Act 1997

Section 313 of the Telecommunications Act sets out the responsibilities and obligations of carriers under the Act. **Item 1 of Schedule 1** inserts **proposed paragraph 313(7)(ca)** to oblige carriers to comply with both the domestic and foreign preservation regimes contained in the TIA Act. These regimes are to be established by the remaining items in this Schedule described below.

42. 'Stored communication' is defined in section 5 of the TIA.
43. 'Carrier' is defined in section 5 of the TIA Act and means carrier (within the meaning of the Telecommunications Act, that is a holder of carrier licence granted under section 56 of that Act) or carriage service provider.
44. Explanatory Memorandum, p. 4.

# Telecommunications (Interception and Access) Act 1979

## Preserving stored communications

**Items 2** to **16** insert definitions into the TIA Act necessary for the drafting of the new provisions dealing with the preservation regime for stored communications. They include definitions of 'preserve' (**item 12**), 'issuing agency' **(item 8**), and 'preservation notice information' (**item 16**). Some of these definitions are discussed below in their relevant context.

**Item 18** inserts a **new Part 3-1A—Preserving stored communications** (**proposed sections 107H** to **107W**) and relates to preserving[45] stored communications held by carriers. In summary, under this new Part 3-1A, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. There are two types of preservation notices: domestic preservation notices (which cover stored communications that might relate either to a contravention of certain Australian laws or to security) and foreign preservation notices (which cover stored communications that might relate to a contravention of certain foreign laws) (**items 3, 4, 10** and **18, proposed subsections 107H(1)** and **107N(1)**).

## Domestic preservation notices

**Proposed sections 107H** to **107M** deal with domestic preservation notices. There are two kinds of domestic preservation notices:

- 'historic domestic preservation notices' (historic notices) which cover stored communications held by the carrier on a particular day (that is the day the notice is received by the carrier)[46] (**proposed subparagraph 107H(1)(b)(i))**, and
- 'ongoing domestic preservation notices', (ongoing notices) which cover stored communications held by the carrier in a particular 30-day period (**subparagraph 107H(1)(b)(ii))**.

**Proposed section 107H** deals with the requirements of a domestic preservation notice. It provides that an 'issuing agency' may give a domestic preservation notice to a carrier that requires that carrier to preserve, while the notice is in force, all stored communications that relate to[47] a specified

45. 'Preserve' means to maintain the integrity of the relevant communication, or a copy of the communication. The phrase 'maintain the integrity' includes ensuring that the relevant information or data is not edited, deleted or otherwise changed (**item 12**).
46. As the Explanatory Memorandum at p.6 notes, a carrier may hold on any particular day stored communications that it received on its systems several days or weeks earlier. Provided the carrier still holds those stored communications on the day on which the historic domestic preservation notice is issued to it, those stored communications must also preserved.
47. **Item 13** inserts a definition of 'relates' which operates differently when the communications relate to a person to when the communications relate to a service. Stored communications relate to a person if the person made or

person or specified communications service(s) and which the carrier holds at any time during the relevant period—the relevant period being a day for historic notices and 30 days for ongoing notices. A notice is usually in force from when the carrier receives it until up to 90 days later (**proposed paragraph 107K(b)(i)).**

An issuing agency for an historic notice is an enforcement agency[48] or ASIO, and an issuing agency for an ongoing notice is an interception agency[49] or ASIO (**subsections 107J(1) and (2))**.)

A preservation notice can only specify one person but may specify more than one telecommunications service (**proposed subsection 107H(3)**).

**Proposed section 107J** sets out the conditions for when an issuing agency can issue each type of domestic preservation notice.

For historic notices, where the issuing agency is an enforcement agency, the agency must be investigating a serious contravention.[50] The agency must also consider that there are reasonable grounds for suspecting that there are, or might be during the relevant period, stored communications that might assist in connection with the investigation; and that there are reasonable grounds for suspecting that there are stored communications which relate to the person or service covered by the notice. The agency must also intend to access the communications with a Part 2-5 warrant or a stored communications warrant[51] if, at a later time, the agency considers such a warrant would be likely to assist in connection with the investigation.

For ongoing notices and where the issuing agency is an interception agency, the conditions for issuing a preservation notice are the same but with the additional limitation that the agency cannot issue another notice if the agency already has a notice in force for that person or telecommunications service.

For domestic preservation notices issued by ASIO, (both historical and ongoing), ASIO must consider that there are reasonable grounds for suspecting that there are, or might be, stored communications which might assist ASIO in carrying out its function of obtaining intelligence relating to security: and that there are reasonable grounds for suspecting that there are stored communications which relate

---

received the communication. Stored communications relate to a particular telecommunications service if the communications has passed over a telecommunications system by way of that service.

48. An enforcement agency for the purposes of Part 3-1A of the TIA Act is a Commonwealth agency (that is the Australian Federal Police, the Australian Commission for Law Enforcement Integrity or the Australian Crime Commission) or an eligible State authority to which a declaration under section 34 is in force (**item 7** and **new paragraph 5(1)(ba)**).
49. An interception agency for the purposes of Part 3-1A of the TIA Act is a Commonwealth agency (that is the Australian Federal Police, the Australian Commission for Law Enforcement Integrity or the Australian Crime Commission) or an eligible state authority (**item 6**).
50. A serious contravention is defined by reference to a penalty of three years imprisonment or more, or 900 penalty units (existing definition in section 5E).
51. The different types of warrants are defined in section 5 of the TIA Act.

to the person or service covered by the notice. Additionally, ASIO must intend to access the communications with a Part 2-2 warrant.[52] ASIO cannot issue another ongoing notice if it already has a notice in force for that person or telecommunications service.

**Proposed section 107KA** identifies the period for which a preservation notice is in force. A notice comes into force when the carrier receives it and ceases to be in force, at the earliest of:

- a 90 day period
- upon receiving a revocation, or
- five days after the issuing of a relevant warrant.

**Proposed section 107M** identifies the persons who can issue or revoke a domestic preservation notice on behalf of an agency.

Domestic notices are automatically revoked after 90 days. They must also be revoked by the issuing agency before that time if the agency is no longer satisfied the grounds for issuing the notice exist, or if the agency decides not to apply for a warrant (**proposed section 107L**).

### Foreign preservation notices

**Proposed sections 107N** to **107S** deal with foreign preservation notices. Foreign preservation notices, like historic domestic preservation notices, cover stored communications held by the carrier on a particular day (**proposed paragraph 107N(1)(b)**).

**Proposed section 107N** provides that if the AFP receives a request to preserve stored communications that is compliant with the conditions set out in **new section 107P**, it *must* issue a foreign preservation notice in relation to those stored communications. The conditions include that the requesting country intends to submit a formal mutual assistance application[53] under new paragraph 15B(d) of the MA Act; that the communications relate to an identified person or telecommunications service and are relevant to a serious foreign contravention (**proposed section 107P**).

A 'serious foreign contravention' is defined as a contravention of the law of a foreign country that is punishable by a maximum penalty of three or more years imprisonment, life imprisonment or the death penalty, or a fine at least equivalent to 900 penalty units[54] (**item 7, proposed section 5EA**).

**Proposed section 107R** deals with revoking a notice.

52. Ibid.
53. A mutual assistance application means an application for a stored communications warrant made as a result of an authorisation under section 15B of the MA Act. (**Item 6, subsection 5(1), Schedule 2**).
54. Under section 4AA of the Crimes Act, one penalty unit is currently $110.

**Proposed section 107Q** provides that a foreign preservation notice comes into force when the carrier receives the notice and ceases to be in force when a revocation under new section 107R is received or a stored communications warrant authorising the disclosure of the communications ceases to be in force.[55] Note that this section contains no default end period[56], the Explanatory Memorandum explaining that this is because the Convention ties the end of preservation to steps within the mutual assistance process (see **proposed section 107R** below).[57]

**Proposed section 107R** provides for the circumstances in which the AFP must revoke a foreign preservation notice. These circumstances are:

> where 180 days have elapsed since the carrier was given the notice and the foreign country did not make a formal mutual assistance request for access to the communications
>
> where the relevant foreign country mutual assistance request is refused by the Attorney-General
>
> where the foreign country withdraws the mutual assistance request.

## Miscellaneous provisions relating to both domestic and foreign preservations notices

**Proposed sections 107T** and **107U,** also inserted by **item 18,** create an evidentiary certificate regime for preservation notices.[58]

**Item 19** inserts **proposed subparagraph 108(2)(f)(ia)**. Its effect is to allow persons to lawfully engage in duties relating to the installation, connection or maintenance of equipment for accessing stored communications in relation to preservation notices.

**Items 21** to **25** relate to the handling and use of 'preservation notice information'.[59]

**Item 23** inserts **proposed subsections 135(4A) and 135(4B)** to create permitted circumstances for dealing with preservation notice information by employees of carriers. The Explanatory Memorandum states that the changes are necessary to maintain the confidentiality of preservation notice information as required by Article 16(3) of the Cybercrime Convention.[60]

**Items 24** and **25** insert the concept of preservation notices in appropriate paragraphs in sections 136, 137, 138 and 139 and 146 of the TIA Act. These insertions allow for the dealing and

55. The TIA Act provides that stored communications warrants are in force for five days before they expire.
56. This is in contrast to the domestic preservation notice provision (contained in **new section 107K**) which has a default end date of 90 days.
57. Explanatory Memorandum, p. 12.
58. Written evidentiary certificates are intended to be conclusive proof of the matters stated in the document.
59. **Item 16** creates the full definition of 'preservation notice information', referred to in **item 7**. The definition is intended to broadly cover anything which could imply the existence of a preservation notice, Explanatory Memorandum, p. 8.
60. Explanatory Memorandum, p. 12.

communication of 'preservation notice information' in the same circumstances as dealing and communication is permitted for stored communications warrant information. This includes the giving of evidence in civil proceedings.

The Explanatory Memorandum states that these changes are necessary to ensure preservation notice information is treated consistently with stored communication warrant information and are necessary to comply with Article 16(3) of the Cybercrime Convention.[61]

**Items 28 to 33** deal with record keeping obligations and include:

- an obligation on the chief officer of enforcement agencies to ensure preservation notices, revocations and evidentiary certificates are kept in each agency's records (**item 28**)
- a role for the Ombudsman in overseeing this record keeping (i**tems 30 and 31**)
- confirmation of the role of the Inspector-General of Intelligence and Security in inquiring into and conducting inspections with regard to the preservation notice scheme (**item 32**)
- an obligation for enforcement agencies and the AFP to include statistics about preservation notices and revocations in their annual reports (**item 33**).

## Comment on Schedule 1

Some of the submissions to the JSC inquiry expressed concerns that the threshold for preservation has been set too low and that the foreign preservation scheme should be part of the more stringent mutual assistance scheme. Both the Explanatory Memorandum and AGD evidence to the JSC inquiry hearings argued against this, stating that the whole purpose of the preservation regime is to act quickly so that data is not destroyed. Because of the urgent nature of preservation, it is best to action preservation requests expeditiously and leave complicated assessments to the full mutual assistance process.

They also make the important point that the data preserved under this regime cannot be accessed without the appropriate warrant which is subject to the conditions of the MA Act.

As the Deputy Director of ASIO argued when giving evidence to the JSC inquiry hearings:

> The key issue there is that we still require a warrant. All the existing oversight mechanisms and procedural processes must be followed to obtain that warrant, approved by the Attorney-General, before we can actually have access to that information. That preservation notice would be given if we had formed an intention to obtain a warrant and we would like that data to be kept in its integrity prior to us obtaining that warrant. But we have no access whatsoever to that information until we have obtained the warrant. That warrant will have to be obtained under all of the existing mechanisms that exist today. There is no additional access to information. There is no backdoor in this. Under this bill, there is no informal way that we would have to obtain

61. Ibid.

> access to that information. We still require the warrant and there is no change to that warrant process under this.[62]

The Commonwealth Ombudsman has other concerns with the preservation scheme and in particular security concerns about carriers' responsibilities under the Act, noting amongst other things that there is a lack of obligation on the carrier to destroy preservation notice information after the 90-days have elapsed or when the notice has been revoked.[63] Their submission suggests a solution would be to ask carriers to certify to the relevant enforcement agency that any product or copies not 'claimed' under a warrant have been destroyed. The Ombudsman should also be responsible for inspecting whether this certification has been kept by enforcement agencies and that it was made in a timely manner. The Ombudsman also argues that there needs to be a clear legislative mechanism to hold carriers accountable for their actions in enabling the execution of stored communications warrants.[64]

Discussions at the JSC inquiry hearings acknowledge that carriers that are bound by the Privacy Act are obliged to destroy information that it no longer required for the purpose for which it was collected.[65] However submitters felt that there should be more specific requirement in the TIA Act so that the data has another layer of protection while it is in that status of being preserved.

The Ombudsman and others also noted that one of the core conditions in the Convention is not included in the Bill, specifically in **new section 107J** of the Bill—that is, the preservation of data should only occur where there is a danger that the data would be modified or lost.

> Those words are in the convention but they are not anywhere in the bill. They really should be the opening criteria for all data preservation notices and we think they should be explicitly set out in the bill.[66]

Ms Smith acknowledged that there is no vulnerability test but suggested that AGD believes that the Convention does not require the Bill to provide further clarification in this respect.

A final point to note about Schedule 1 relates to the domestic preservation notice regime which provides for ongoing collection and retention of communications (**proposed section 107H**). This ongoing collection, while only applicable to domestic notices, is not provided for by the Convention. Similarly the scheme extends to ASIO, and this is not a requirement of the Convention but has been done on the basis of 'interoperability' with law enforcement agencies. In discussions on the Bill at the JSC inquiry hearings about the domestic security and enforcement agencies access to the

---

62. D Fricker (Deputy Director ASIO), Joint Select Committee on Cyber-Safety, *Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 25.
63. Commonwealth Ombudsman, op. cit., p. 5.
64. Ibid.
65. However while the Privacy Act applies to carriers and carriage service providers, the small business exemption under the Act means that a large number of Internet Service Providers would be exempt from the Privacy Act.
66. C Connolly (Research Associate, CLPC), Joint Select Committee on Cyber-Safety, *Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 13.

preservation regime, the Deputy Director of ASIO stated the extension was on the principle that the additional security benefits that would be extended to criminal investigations should be afforded to Australia's security considerations as well.

> It is just the simple logic [...] that it would not make sense to construct these arrangements in those regimes to protect one aspect of Australia's security while overlooking the opportunity it has to further ASIO's role in national security.[67]

## Schedule 2 – Amendments relating to mutual assistance

### Overview

The amendments in **Part 1** of **Schedule 2** seek to amend the MA Act and the TIA Act so that following a formal mutual assistance request from a foreign country, the Attorney-General may authorise the AFP or a state police force to apply for a stored communications warrant to assist in the investigation of a foreign offence.

The amendments in **Part 2** of **Schedule 2** seek to:

- amend the TIA Act to allow the AFP to obtain historical telecommunications data from a telecommunications carrier and to pass that data on directly to a foreign law enforcement agency without the need for a formal request to be made by the foreign country under the Mutual Assistance Act, that is, on an agency to agency basis.
- amend the Mutual Assistance Act and the TIA Act to enable the collection of prospective telecommunications data for foreign law enforcement purposes. The amendments would only enable this type of assistance to be provided where the country has made a mutual assistance request and the Attorney-General has authorised provision of the assistance.

The Explanatory Memorandum states that the amendments in this Schedule relate to Australia's obligations under Articles 30, 31, and 33 of the Convention.[68] Article 31 provides for access for foreign countries to stored computer data. Article 30 provides for access for disclosure of traffic data—that is telecommunications data— to foreign countries to enable the identification of service providers and the path of a communication. Article 33 provides for mutual assistance to foreign countries in the real-time telecommunications data. Further, Article 33 requires the assistance to be provided with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

67. D Fricker (Deputy Director ASIO), op. cit., p. 27.
68. Explanatory Memorandum, p. 16.

# Part 1—Stored communications warrants

## Mutual Assistance in Criminal Matters Act 1987

**Items 1 to 4** amend the MA Act. The key amendment is **item 4** which inserts **new Part IIIA** containing **proposed section 15B** and relates to obtaining a stored communications warrant for foreign law enforcement purposes. It is a significant provision and will enable the Attorney-General to authorise the AFP or state of territory police to apply for a stored communications warrant under section 110 of the TIA Act if:

- a request for access to the stored communications has been received from a foreign country
- an investigation or investigative proceeding[69] relating to a criminal matter involving an offence against the law has commenced in the requesting country
- the offence to which the investigation or investigative proceeding relates, is punishable by a maximum penalty of three or more years imprisonment, life imprisonment or the death penalty, or a fine equivalent to, or greater than 900 penalty units[70] and
- there are reasonable grounds to believe that a carrier holds stored communications relevant to the investigation or investigative proceeding.

A note to this provision states that information obtained under the warrant may only be communicated to the requesting country on certain conditions and that these conditions are set out in **new subsection 142A(1)** of the TIA Act (to be inserted by **item 20)**. These conditions are that the information will only be used for the purposes it was requested, that the material will be destroyed when no longer required for those purposes, and any other conditions determined by the Attorney-General.

**Items 1** to **3** insert definitions of 'carrier', 'investigative proceeding' and 'stored communication'. The definitions of 'carrier', and 'stored communication' have the same meaning as in the TIA Act.

## *Telecommunications (Interception and Access) Act 1979*

**Items 5** to **34** of **Schedule 2** contain amendments to the TIA Act.

**Items 9** to **14** amend section 116 that deals with the issuing of stored communications warrants. Under section 116 prescribed Australian enforcement agencies may apply to an 'issuing authority'[71] for a warrant to covertly access stored communications to assist in the investigation of domestic offences. The enforcement agency's investigation must relate to a domestic offence that is punishable by imprisonment for at least three years or a fine of at least 180 penalty units for an

69. Defined in **subsection 3(1), item 2**.
70. Under section 4AA of the Crimes Act, one penalty unit is currently $110.
71. 'Issuing authority' is defined in section 6DB of the TIA Act as a judge, magistrate and certain AAT members.

individual or 900 penalty units for a corporation.[72] **Item 9** will amend **section 116** with the effect of facilitating the issue of a stored communications warrant in response to a mutual assistance application, (that is for the investigation of a foreign offence on behalf of a foreign country.[73] Under **proposed paragraph 116(1)(d)(ii)** the issuing authority will be required to be satisfied, that information likely to be obtained under the warrant would be likely to assist in the investigation of a serious foreign contravention[74] in which the person is involved.

Existing subsection 116(2) lists certain factors that an issuing authority must have regard to when determining whether to issue a stored communications warrant. **Item 13** inserts **proposed subsection 116(2A)** and sets out the matters to which an issuing authority must have regard when determining an application for a stored communications warrant made with regard to a mutual assistance request. These matters are:

- the likely interference with any person's privacy
- the gravity of the conduct constituting the serious foreign contravention, and
- how much the information obtained by accessing the stored communication would assist in connection with the foreign investigation, to the extent this can be determined.

Existing section 139 of the TIA Act sets out some of the permitted dealings with lawfully accessed information[75] or stored communications warrant information.[76] **Item 19** inserts **proposed subsection 139(4A)** and sets out the purposes for which information obtained through the execution of a warrant issued as a result of a mutual assistance application can be used. These purposes include transmission of information to the foreign country and for record keeping requirements. **Items 17** and **18** are consequential to this amendment.

As noted earlier, **item 20** inserts **proposed section 142A** and sets out 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 only be used for the purposes for which the foreign country requested the information
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes, and
- any other condition determined, in writing, by the Attorney-General.

72. Under section 4AA of the Crimes Act, one penalty unit equates to $A110.
73. A definition of a 'mutual assistance application' is inserted by **item 6**.
74. See above at p. 12.
75. 'Lawfully accessed information' is defined in subsection 5(1) of the TIA Act as information obtained by accessing a stored communication.
76. 'Stored communications warrant information' is defined in subsection 5(1) of the TIA Act

Currently, sections 161 to 163 of the TIA Act require the Minister to prepare an annual report containing statistics on the use of stored communications warrants. **Items 21** to **23** amend **section 162** to add reporting obligations relating to mutual assistance applications for warrants.

## Comment on Part 1—Amendments relating to stored communications warrants

Issues of dual criminality have already been referred to in the Main issues section above.

Submitters to the JSC inquiry raised other issues about Part 1 and the new stored communications warrant regime.

One of these issues relates to **proposed subsection 116(2A)** of the TIA. As noted above this provision sets out a threshold test for obtaining a stored communication warrant to assist in the investigation of a foreign offence. The test is:

- the likely interference with any person's privacy
- the gravity of the conduct constituting the serious foreign contravention, and
- how much the information obtained by accessing the stored communication would assist in connection with the foreign investigation, *to the extent this can be determined*.

Some submissions note that the new threshold test to apply to foreign requests is less onerous than the one for the issuing of a domestic investigation warrant (existing subsection 116(2)).

In relation to the third dot point (*how the information obtained would assist with the foreign investigation*), the Law Council argues there is no justification for diluting this important threshold test with the phrase 'to the extent this can be determined'. It states:

> If foreign agencies want to be able to employ intrusive police powers, which impact directly on the privacy of those targeted, in the context of their investigations, they ought to be required to provide sufficient information to allow the merits of their request to be properly tested. Such information should clearly include well supported claims about the likely value of the evidence or information sought to be obtained.[77]

By way of comparison the Law Council also noted that the threshold test for the issuing of a *domestic* investigation warrant contains additional factors to be considered namely:

- to what extent methods of investigating the relevant offence that do not involve the use of a stored communications warrant have been used or are available
- how much the use of such methods would be likely to assist in connection with the investigation by the agency of the relevant offence, and

77. Law Council of Australia, op. cit., p. 5.

- how the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reasons.

These threshold considerations are intended to underscore the fact that covert access to stored communications should only be authorised when more conventional and less intrusive investigative techniques have proven, or are likely to prove, ineffective or impractical.[78]

However these factors are considerations for a domestic investigation warrant but not for a foreign warrant.

The Explanatory Memorandum justifies the omission of these factors in relation to foreign country requests, stating that the additional factors relate to knowledge that it is only feasible for the enforcement agency making the application to possess in relation to a domestic contravention. Therefore it is not appropriate for these matters to be included as relevant consideration in issuing a foreign investigation warrant.[79]

## Part 2 – Amendments relating to telecommunications data

### Mutual Assistance in Criminal Matters Act 1987

**Items 25 to 27** amend the MA Act. The main amendment is **item 27** that inserts **new Part IIIB – Assistance in relation to telecommunications data** and contains **proposed section 15D**. **Proposed subsection 15D(3)** states that the Attorney-General may make an authorisation allowing a foreign country access to telecommunications data under **new section 180B** of the TIA Act 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 the death penalty.

The section only applies to foreign country requests for prospective telecommunications data (**proposed subsection 15D(1)**) and authorisations will not extend to the contents or substance of a communication (**proposed subsection 15D(2)**).

**Items 25** and **26** insert definitions of 'communication' and 'telecommunication system' relying on definitions in the TIA Act.

78. Ibid., p. 6.
79. Explanatory Memorandum, p. 25.

### *Telecommunications Act 1997*

**Items 28 to 31** amend **sections 306** and **306A** of the Telecommunications Act and insert record keeping obligations in relation to the new authorisation regime for disclosure of telecommunications data for foreign law enforcement purposes.

### Telecommunications (Interception and Access) Act 1979

**Items 32** to **53** amend the TIA Act.

**Item 41** inserts a **new Division 4A—Foreign law enforcement** into Part 4-1 of the TIA Act. It is a key amendment and provides the basis for historical (ie existing) and prospective telecommunications data to be provided to a foreign country for foreign law enforcement purposes. It is divided into:

- Subdivision A—Primary disclosures (containing proposed sections 180A and 180B)
- Subdivision B—Secondary disclosures (containing proposed sections 180C and 180D)
- Subdivision C—Conditions of disclosure to foreign country (containing proposed section 180E).

**Proposed section 180A** provides the basis for the AFP to authorise the disclosure of historical telecommunications data to a foreign country for the purposes of the enforcement of the criminal law of a foreign country. (Historical data is existing data or data that came into existence before the disclosure request is received).

**Proposed subsection 180A(2)** provides that an authorised officer of the AFP[80] may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation. Under **proposed subsection 180A(3**), an authorised AFP 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. **Proposed subsection 180A(4**) provides that where specified information or documents have been disclosed because of an authorisation under subsection 180A(2), the authorised officer of the AFP may authorise the disclosure to the foreign law enforcement agency[81], but only if satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country and the disclosure is appropriate in all the circumstances.

**Proposed section 180B** deals with authorisations for access to *prospective* information or documents. This provides much wider scope for sharing of data and accordingly the conditions are more restrictive.

80. An 'authorised officer' is defined as the AFP Commissioner and Deputy Commission or a senior executive AFP officer who has been authorised in writing by the AFP Commissioner (**subsection 5(1),** amended by **item 32**).
81. A 'foreign law enforcement agency' is a police force of a foreign country or any other authority or person responsible for the enforcement of the laws of the foreign country (**item 33**).

Under **proposed section 180B** prospective telecommunications data will only be able to be provided to a foreign country where the country has made a mutual assistance request and has been authorised by the Attorney-General.

**Proposed subsection 180B(2)** provides that an authorised AFP officer may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force. **Proposed subsection 180B(3)** provides that an authorised officer will only be able to make an authorisation if:

- the Attorney-General has authorised it under section 15D of the MA Act (inserted by **item 27**), and
- the officer is satisfied that the disclosure is:
  - reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and
  - appropriate in all the circumstances.

Authorisations made under this section will be in force for up to 21 days with a possible extension of another 21 days (**proposed subsections 180B(5)** to **(7)**).

**Proposed subsection 180B(8)** provides that when information or documents are disclosed to the AFP as a result of an authorisation under subsection 180B(2), an authorised AFP officer may then disclose the documents or information to a foreign law enforcement agency providing the authorised officer is satisfied that the disclosure is:

- reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and
- appropriate in all the circumstances.

**Proposed sections 180C** and **180D** deal with secondary disclosures.

**Proposed section 180C** will allow information or documents disclosed because of an authorisation under sections 178, 179 and 180 of Division 4 (that is disclosures for domestic purposes)[82], to also be disclosed to a foreign law enforcement agency providing the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country and the disclosure is appropriate in all the circumstances.

**Proposed section 180D** will allow information or documents disclosed because of an authorisation under new Division 4A for foreign purposes, to also be used by the AFP, or further disclosed to ASIO

82. Except for information disclosed under section 178A (that is missing person information).

or to another enforcement agency for domestic purposes. These secondary disclosures will be subject to the conditions set out in **proposed subsection 180D(2).**

**Proposed section 180E** imposes additional conditions on when information or documents can be disclosed to a foreign country under new section 180A, 180B or 180C. These conditions are:

- that the information will only be used for the purposes for which the foreign country requested the information
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes, and
- in the case of section 180B (that is prospective information or documents), any other condition determined, in writing, by the Attorney-General.

**Item 41** also inserts new **Division 4B—Privacy to be considered when making authorisations** and consists of **proposed section 189F**. This provision require an authorised officer, prior to making any authorisation (for either domestic and foreign purposes) to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure or use.

This provision mirrors existing **subsection 180(5)** which is to be repealed by **item 40**. Subsection 180(5) currently imposes privacy conditions only in relation to domestic purpose authorisations whereas new section 189F will provide that privacy considerations are taken into account for every disclosure of historical and prospective telecommunications data under Division 4 and 4A of Part 4-1 of the TIA Act.

**Items 42** and **43** amend **section 182** of the TIA adding references to **Division 4A** into an offence provision to do with further disclosure or use of telecommunications data or information. The effect will be to make it an offence to further use or disclose information originally disclosed as permitted by Division 4A.

**Items 45** to **50** amend provisions dealing with the technical requirements of authorisations and notifications to include a reference to the new regime relating to authorisations to foreign countries as set out in Division 4A. The effect will be, for example, that:

- the Commissioner of the AFP will be required to retain each authorisation made under new Division 4A for three years (**item 49**)
- the AFP will be required to include in their report to the Minister the number of authorisations made under new sections 180A, 180B, 180C and 180D in that year (**item 50**).

These record-keeping requirements already apply to disclosure authorisations under existing Division 4.

## Comment on Part 2—Amendments relating to telecommunications data

The reader is referred to the Key issues section for additional comment on this Part.

A further point of note relates to **proposed section 180A** of the TIA Act that allows the AFP to pass historical telecommunications data to their foreign counterparts without the need for a mutual assistance request. The Government's rationale is that this will be a less-time consuming process.[83]

This process has raised concerns relating to human rights. Whereas the MA processes have limitations that restrict co-operation with foreign countries in cases where the particular offence being investigated is a political offence, or is otherwise inconsistent with fundamental human rights standards, this is not reflected in the process for agency-to-agency transfers being proposed in section 180A. Furthermore, there is no restriction on the number or type of countries that may receive telecommunications data from the AFP, for example non-signatories of the Convention. The Australian Privacy Foundation argues that it is essential that a Bill to enable accession to the Convention not encompass all 'foreign countries' and that provisions relating to preservation and/or access to data on behalf of foreign countries must be explicitly restricted to Contracting Parties to the Convention.[84]

It has also been noted that there is no independent oversight of compliance with police authorised disclosures and none envisaged in relation to disclosure to foreign counterparts.[85]

## Schedule 3— Criminal Code Amendments

### Criminal Code Act 1995

Computer-related offences in Australia are set out in Commonwealth as well as state and territory law. At Commonwealth level the offences are contained in Part 10.7 of the Criminal Code Act. These offences are based on model laws developed by the Model Criminal Code Officers Committee in 2001. The offences cover acts relating to illegal access, modification and impairment of computer data.

In their current form, and for Constitutional reasons, the computer offences in Part 10.7 are restricted to conduct involving Commonwealth computers, Commonwealth data or the use of a carriage service. For situations not covered by Commonwealth laws, state and territory offences are used by law enforcement agencies.

The Explanatory Memorandum states that these limitations are not consistent with the obligations in the Convention.

83. Explanatory Memorandum, p. 16.
84. Australian Privacy Foundation, op. cit., p. 7.
85. The Australian Privacy Foundation argues that it is essential that a Bill to enable accession to the 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 (sic) transparency to the public'. Australian Privacy Foundation, op. cit., p. 9.

> Although state and territory offences provide some coverage for conduct which is excluded from the Commonwealth offences, some gaps remain. To ensure that Australia can meet the obligations under the Convention, this Schedule will remove the current restrictions on the computer offences in Part 10.7.[86]

For example, **subsection 477.1(1)** of the Criminal Code Act provides that it is an offence to cause unauthorised access to or unauthorised modification of data held in a computer, or unauthorised impairment of electronic communication to or from a computer with intent to commit a serious offence. **Paragraph 477.1(1)(b)** currently limits the offence to situations where the unauthorised access, modification or impairment is caused by means of a carriage service. **Item 2** will remove this limitation to a carriage service. **Subsection 477.1(4)** provides that it is an offence to cause unauthorised access to data held within a computer, unauthorised modification of data held in a computer, or unauthorised impairment of electronic communication to or from a computer with intent to commit a serious Commonwealth offence. **Item 4** will remove this requirement of intention to commit a serious Commonwealth offence.

**Subsection 477.2(1)** provides that it is an offence to cause unauthorised modification of data held in a computer in order to impair access to that or any other data or to impair the reliability, security or operation of any such data. **Paragraph 477.2(1)(d)** currently limits the offence to situations involving or affecting a carriage service, a Commonwealth computer or data held on behalf of the Commonwealth in a computer. **Items 5, 6** and **7** will amend **subsection 477.2** with the effect of removing these limitations—that is, removing the existing requirement:

- for a carriage service to have been used
- for a Commonwealth computer to have been involved or affected, or
- for data held on behalf of the Commonwealth in a computer to have been affected, in the commission of the offence.

The remaining items in this Schedule (**items 8** to **17**) make similar amendments. That is, they remove references to a carriage service and to Commonwealth computers or Commonwealth data, the effect being to broaden the offence provisions and remove limitations so that the computer-related offences in Part 10.7 of the Criminal Code Act have coverage beyond Commonwealth involvement and beyond the use of carriage services.

## Comment on Schedule 3 and the Criminal Code amendments

One of the effects of Schedule 3 would be that the existing computer offences in the Criminal Code Act would no longer need to have a nexus with the Commonwealth, for example through being concerned with data held in a Commonwealth computer or with the use of a carriage service. Furthermore, such an expansion of the scope of federal criminal offences in this area would mean

86. Explanatory Memorandum, p. 47.

that there would be a significant degree of overlap between the Commonwealth's computer offences and state existing computer offences.[87]

The provisions in Schedule 3 have raised concerns about their impact on the interrelationship between Commonwealth and state criminal laws.

Submissions to the JSC inquiry raised concerns about the impact of the Schedule 3 amendments on the interrelationship between Commonwealth and state computer offences.

The Attorney-General, in his second reading speech, argues the new arrangements will not cause constitutional difficulties, stating that the amended powers will be supported by the external affairs power—Australia implementing this legislation as part of its compliance with an international treaty obligation. The Attorney-General further argues that in the event of any inconsistency between Commonwealth and state or territory laws, the savings provisions contained in the Criminal Code (existing section 476.4) will ensure the validity of those state and territory laws.[88]

However several submissions, including that of Dr Jeremy Gans, and two state Governments argue the Bill's provisions could have constitutional consequences as a result of a recent High Court judgement, *Dickson v R.*[89] In that decision the High Court invalidated certain Victorian legislative provisions in so far as they were held to be inconsistent with certain provisions of the Commonwealth Criminal Code Act dealing with the same subject matters (conspiracy to steal Commonwealth property). The Victorian Attorney-General's submission notes that the High Court in its reasons appeared to take a broader view of what counts as constitutional inconsistency than many had previously expected and that this has had the effect of introducing a notable degree of uncertainty into the constitutional law governing overlapping criminal laws.[90]

The submission notes that the full impact of the *Dickson* decision is yet to be determined and that it is anticipated that the High Court's pending decision in *Momcilovic v Queen* may help to clarify the law in this area.[91]

The Victorian Attorney-General acknowledges that the Bill is not intended to alter the current section 476.4 of the Commonwealth's Criminal Code, which purports to prevent the Code's computer offences from excluding or limiting the operation of state or territory Laws. However he expresses caution stating:

87. For example, sections 247A to 247I of the Crimes Act 1958 (Vic).
88. R McClelland, 'Second reading speech: Cybercrime Legislation Amendment Bill 2011', House of Representatives, *Debates*, 22 June 2011, p. 6822, viewed 15 August 2011, http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/d78cdc58-c20e-4fbf-a147-88f30644229d/0012/hansard_frag.pdf;fileType=application%2Fpdf
89. (2010) 241 CLR 491, [2010] HCA 30.
90. R Clark, op. cit.
91. Ibid. This decision is currently reserved.

> Be that as it may, such a clause is by no means guaranteed to protect Victorian or other State laws if the High Court were to find that any such laws in this area were directly inconsistent with a Commonwealth law.[92]

The submission therefore concludes:

> Until the High Court's approach to the criteria for identifying inconsistency in the area of overlapping State and federal criminal offences is made clearer, the prudent course would be for the Commonwealth Parliament to avoid risking unintended consequences by expanding the scope of Commonwealth criminal law without yet knowing the effects of such a step. In the meantime, the States and the Commonwealth can continue to work together to ensure that the substantive law within Australia provides an effective tool in the combating of cybercrime.[93]

Dr Geremy Gans, from the University of Melbourne Law School, takes a slightly different view. He believes *Dickson* already poses a potential problem for most state computer offence prosecutions and he also agrees that the Bill would widen the area of overlap between Commonwealth and state offences (and, hence, the area of possible invalidity of state offences). That is, the state prosecutions that will be potentially invalid once the Bill has passed will include computer offences that involve neither federal crimes, federal computers nor the internet. However Dr Gans does not see the *Dickson* problem as any reason not to pass the Bill and argues that whatever damage has been wrought by *Dickson* has already largely been done by the enactment of Division 477 (and mirroring state legislation) in the first place.[94]

In response to questions about this issue at the inquiry hearings the AGD officer acknowledged the potential problems caused by *Dickson* and the difficulty of speculating the outcome in *Momcilovic v the Queen* but also pointed out that the effect of the Bill will be very minimal on Commonwealth and state offences. Ms Chidgey states:

> Our approach is that we have done everything we can to preserve the concurrent operation of all the state and territory laws.
>
> [...]
>
> In a worst case scenario, where the High Court found that the Commonwealth and state offence regimes covering the same subject matter were slightly different, it would mean the Commonwealth and the states and territories having to consider their approach across all drug offences or money-laundering offences—a whole range of areas. The change that this bill is making in computer offences is a very, very small change, so I do not think this affects that position at all.[95]

92. Ibid.
93. Ibid.
94. Division 477 of the Criminal Code Act relates to serious computer offences.
95. S Chidgey, (Assistant Secretary, Criminal Law and Enforcement Branch, AGD), Joint Select Committee on Cyber-Safety, *Cybercrime Legislation Amendment Bill 2011*, Hansard, 1 August 2011, [proof copy], p. 33.

## Schedule 4—Telecommunications data confidentiality

### Overview

Schedule 4 contains amendments to the TIA Act aimed at keeping confidential the existence of authorisations for the disclosure of information or documents made under Chapter 4—Access to telecommunications data of the TIA Act.

### Telecommunications (Interception and Access) Act 1979

**Item 3** inserts **proposed sections 181A** and **181B** into the TIA Act. These new section create offences relating to the use or disclosure of information that relates to authorisations.

**Proposed section 181A** relates to authorisations made under Division 3 of Chapter 4 of the TIA Act. These are authorisations made by ASIO for the disclosure of documents that relate to ASIO's performance of its function of obtaining intelligence relating to security.

**Proposed subsection 181A(1)** creates an offence if a person *discloses* information which is about:

- whether an authorisation under Division 3 (other than under section 178A)[96] has been, or is being, sought
- the making of such an authorisation
- the existence or non-existence of such an authorisation
- the revocation of such an authorisation, or
- the notification of such a revocation.

**Proposed subsection 181A(2)** creates an offence if a person *discloses* a document to a person and the document consists (wholly or partly) of any of the following:

- an authorisation under Division 3
- the revocation of such an authorisation, or
- the notification of such a revocation.

The maximum penalty for the offences in subsections 181A(1) and (2) is two years imprisonment.

**Proposed subsection 181A(3)** provides exemptions for these offences where:

- the disclosure is for the purposes of the authorisation, revocation or notification concerned, or
- the disclosure is reasonably necessary:
- to enable ASIO to perform its function of obtaining intelligence relating to security
- to enforce the criminal law

96. That is missing person information.

- to enforce a law imposing a pecuniary penalty, or
- to protect the public revenue.

**Proposed subsections 181A(4) and 181A(5)** create offences relating to *the use* of the same information and documents set out in new subsections 181A(1) and (2). **Proposed subsection 181A(6)** creates exemptions to these offences, so that ASIO can make use of the authorisations that they have made.

**Item 3** also inserts **proposed section 181B** and deals with offences relating to the disclosure and use of authorisations made under Division 4 of Chapter 4 of the TIA Act. These are authorisations made by enforcement agencies for the purposes of enforcing the criminal law; enforcing a law imposing a pecuniary penalty; or protecting the public revenue.

The offences relate to the same activities set out in new section 181A and the exemptions to these offences mostly mirror those contained in new section 181A.

### Comment on Schedule 4

These amendments are in part a response to Convention obligations which places requirements on Parties to adopt legislative and other measures to keep confidential the execution of powers provided for by the Convention, as well as the information obtained from the use of those powers.

However the amendments go beyond Convention obligations as they impose confidentiality requirements on the information contained in the actual instruments authorising access to telecommunications data under Chapter 4 of the TIA Act. The Explanatory Memorandum states that the rationale for this extension is:

> In addition to facilitating accession to the Convention, these provisions will increase the operational security provided by the TIA Act. Given that the use of authorisations is one of the main methods of identifying relevant services related to telecommunications interception and stored communications warrants, it is important to ensure that protections are in place across the life of an operation.[97]

## Concluding comments

Undoubtedly cybercrime is an increasing and challenging threat and many see the Convention with its aims of developing a common criminal policy and promoting international cooperation as a way of responding to those challenges.

97. Explanatory Memorandum, p. 52.

The provisions in the Bill are complex as they set up new arrangements that cut across several areas of law, including criminal law, mutual assistance legislation and laws relating to telecommunications interception and stored communications data.

The Bill is also controversial as indicated in submissions to the JSC inquiry with many civil liberties groups and legal and regulatory bodies expressing concerns. While the Bill does contain a number of important protection and accountability mechanisms many submissions argue that at the very least the Bill needs attention to improve the rigour of the various threshold tests, reporting obligations and privacy safeguards.

The challenge for the Parliament is to ensure that the Bill strikes an appropriate balance of the right to privacy and the protection of human rights with the policy objectives associated with the implementation of the Convention. As the Law Council has commented the form of the amendments is in no way dictated by the Convention and the Government (and the Parliament) is not constrained by the Convention in responding to and addressing the concerns raised in submissions.

Another point of note is that while the stated purpose of the Bill is to facilitate Australia's accession to the Convention, in some respects the Bill does go beyond Convention obligations—for example by extending the preservation notice scheme to ASIO and by extending the new arrangements beyond signatories to the Convention—the rationale being to ensure interoperability between security and law enforcement agencies and to increase operational security provided by the TIA Act. A final point of interest is that while commencement of the Criminal Code amendments in Schedule 3 is tied to Australia's accession to the Convention, the remaining provisions commence 28 days after Royal Assent, irrespective of whether and when Australia accedes to the Convention.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2438.