Law Council
OF AUSTRALIA

Cybercrime Legislation Amendment Bill 2011

Joint Select Committee on Cyber-Safety

14 July 2011

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Introduction

1. The Law Council welcomes the opportunity to respond to the Joint Select Committee on Cyber-Safety's inquiry into the *Cybercrime Legislation Amendment Bill 2011* ('the Cybercrime Bill').

2. The purpose of this Bill is to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Criminal Code Act* 1995, the *Mutual Assistance in Criminal Matters Act 1987* (the Mutual Assistance Act) and the *Telecommunications Act 1997* to ensure that Australian legislation is compliant with the Council of Europe's Convention on Cybercrime (the Convention) in order to facilitate Australia's accession to the Convention.[1]

3. The Law Council has a number of concerns about the amendments proposed in Schedule 2 of this Bill, and submits that these proposed amendments require further consideration and revision before they are enacted.

4. The amendments contained in Schedule 2 are primarily concerned with whether, how and in what circumstances Australian law enforcement authorities may obtain access to and share information about stored communications (such as text messages, voice messages and emails) or telecommunications data (such as telephone subscriber details and records about to whom calls were made, when and from where) to assist in the investigation of a foreign offence.

5. The amendments were first proposed by the Government in an exposure draft of the *Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill* released by the Attorney-General's Department in 2009. The proposed amendments were again included in a revised exposure draft of the same legislation released earlier this year.

6. On both occasions the Law Council made submissions to the Department indicating that it did not object to the aims of the amendments in principle. However, 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.

7. These concerns have not been addressed in the current Bill and are therefore set out again below for the benefit of the Committee.

8. The Law Council submits that until these concerns are addressed the relevant provisions should not be enacted.

9. In that regard, it is 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 below.

[1] Explanatory Memorandum to Cybercrime Legislation Amendment Bill 2011, p.1

Stored communications warrants: threshold tests, reporting obligations and privacy safeguards

10. Schedule 2, Part 1 of the Cybercrime Bill seeks to amend the Mutual Assistance 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.

11. The Law Council does not object to the aim of these amendments, but submits that if covert and intrusive police powers of this kind are to be made available to assist in the investigation of foreign offences, then the following minimum requirements should apply:

    i. Before issuing a warrant or authorising the disclosure of information, the relevant officer must be satisfied of precisely the same matters that he or she would be required to be satisfied of if the information were sought in the context of a domestic investigation (e.g. seriousness of the offence, necessity, privacy, likely benefit etc.);

    ii. The reporting requirements in relation to:

        1. The number of warrants applied for and granted;
        2. The type of investigations (i.e. the types of offences) for which the information was sought; and
        3. The use made of information obtained under the warrant,

        must be the same as they are for warrants obtained in the context of a domestic investigation; and

    iii. The restrictions placed on the use, disclosure, retention and destruction of information obtained under the warrant must mirror those that would be in place if the warrant was sought in the context of a domestic investigation.

12. The proposed amendments in the Cybercrime Bill do not fully comply with these requirements. Indeed, in several respects, the threshold test and reporting requirements in relation to information sought in the context of a foreign investigation are not as stringent.

<u>Threshold test for obtaining a stored communications warrant</u>

13. The Law Council has three primary concerns with the proposed threshold test for obtaining a stored communication warrant to assist in the investigation of a foreign offence.

    - The proposed provisions state that a stored communication warrant may only be applied for in the context of a foreign investigation which relates to an offence carrying a maximum penalty of imprisonment for 3 years or more, imprisonment for life, the death penalty, or a fine of an amount that is at least equivalent to 900 penalty units.

These provisions seek to ensure that stored communications may only be obtained under warrant and provided to assist in the investigation of a foreign offence if the offence concerned is of a prescribed level of seriousness.

The Law Council is concerned that under the proposed amendments, the seriousness of the offence being investigated and whether it meets the required threshold test is measured by reference to the maximum penalty imposed for the offence in the requesting country. Such penalties may be considerably out of sync with, and much more severe than, the penalties imposed in Australian jurisdictions for like conduct.

The Law Council therefore submits that the relevant provisions should be amended to require that the offence under investigation would attract the requisite threshold penalty had it been committed in Australia.

It should not be possible under the Mutual Assistance Act and 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.

- Under the existing provisions of the TIA Act, one of the matters that an issuing authority is required to consider before issuing a stored communications warrant in the context of a domestic investigation is "*how much the information (sought to be obtained) would be likely to assist in connection with the investigation."*[2]

  However, in the current Bill, it is proposed that when a stored communications warrant is sought in the context of a foreign investigation, the likely value of the information sought to be obtained by the warrant will only be required to be assessed by the issuing authority to the extent that the information provided by the requesting country allows for such an evaluation.[3]

  The Law Council submits that there is no justification for the dilution of this important threshold test. 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.

- Under the existing provisions of the TIA Act, further matters that an issuing authority is required to consider before issuing a stored communications warrant in the context of a domestic investigation warrant include:

  - to what extent methods of investigating the [relevant offence] that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency seeking the warrant; and

  - 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

[2] *Telecommunications (Interception and Access) Act 1979*, s 116(2)(c)
[3] Proposed subsection 116(2A)(c) (see item 13 in Schedule 2 of the Bill).

- 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 reason.[4]

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.

However, in the current Bill, the issuing authority will not be required to consider any of these matters where a stored communications warrant is sought in the context of a foreign investigation. The Law Council submits that there is no justification for exempting warrant applications which relate to foreign investigations from this important necessity test.

As above, 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 information about why resort to a stored communications warrant is necessary in the circumstances of their particular investigation.

Reporting requirements for stored communications warrants

14. Under the existing provisions of the TIA Act, where a stored communications warrant is issued in the context of a domestic investigation, the agency which obtains the warrant is required to capture and report on information about the number and type of arrests made, prosecutions instituted and convictions secured as a result of the information obtained under the warrant.[5] This type of reporting is useful in allowing review and scrutiny of whether the information provided, and claims made, in warrant applications were actually borne out by the results obtained.

15. It appears that the same reporting requirements are not proposed in relation to stored communications warrants issued in the context of a foreign investigation.

16. The Law Council submits that there is no justification for this proposed gap in reporting.

17. If foreign agencies want to have access to intrusive investigative powers, it would appear reasonable to require that they provide feedback data on how they have used the information obtained. Only in this way can Australian authorities satisfy themselves, on an ongoing basis, about the reliability, necessity and likely utility of future warrant requests.

Restrictions on use, disclosure, retention and destruction of information obtained under a stored communications warrant

18. Proposed section 142A of the TIA Act (see item 20 of Schedule 2) provides that a person may only communicate information, obtained through the execution of a warrant issued as a result of a mutual assistance application, to the foreign country to which the application relates, subject to the following conditions:

[4] *Telecommunications (Interception and Access) Act 1979*, s 116(2)(d)–(f)
[5] *Telecommunications (Interception and Access) Act 1979*, s 163

- 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;

- any other condition determined, in writing, by the Attorney-General.

19. The Law Council supports the proposal to impose conditions of this type on the transfer of information. However, the Law Council queries how, in the absence of an undertaking, these conditions would 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.

20. As a result of the uncertainty about the effectiveness of these privacy protection arrangements in practice, the Law Council submits that sub-section 8(2) of the Mutual Assistance Act should 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 assistance where the requesting country's arrangements for handling personal information (whether legislative, contractual, or otherwise) do not offer privacy protections substantially similar to those applying in Australia.

Authorisation to disclose Telecommunications Data – Threshold Tests, Reporting Obligations and Privacy Safeguards

21. Schedule 2, Part 2 of the Cybercrime Bill seeks 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.

22. As above, the Law Council does not object to the aim of these amendments. However, again, the Law Council submits that more stringent tests and conditions should be imposed before the relevant information is able to be accessed and disclosed.

<u>Threshold test for authorising the disclosure of telecommunications data</u>

23. Under the proposed provisions of the Bill, Australian law enforcement authorities will be able to authorise the disclosure of historical telecommunications data to assist in the investigation of a foreign offence and to provide that information directly to their

counterparts overseas, without the need for the Minister to first receive, scrutinise and approve a formal mutual assistance request.

24. While telecommunications data does not include the content and substance of a person's private communications, it nonetheless may reveal information about crucial and private matters such as a person's associations and movements. Therefore strict conditions should attach to the disclosure and use of such information.

25. Although the Law Council does not object in principle to amendments which would allow historical telecommunications data to be obtained and shared on an agency to agency basis, appropriate safeguards must be imposed to ensure that the types of matters which would have been taken into account in evaluating a mutual assistance request are also given due consideration by law enforcement agencies before providing assistance on an agency to agency basis.

26. The Law Council submits that the Bill in its current form does not make adequate provision for such safeguards.

27. Proposed sections 180A(5) and 180C(2) of the TIA Act provide that an authorised officer must not authorise the disclosure of telecommunications data to a foreign law enforcement agency (whether it was obtained specifically for the purpose of assisting in a foreign investigation or whether it was originally obtained in the context of a domestic investigation) unless he or she is satisfied that:

    (a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and

    (b) the disclosure is appropriate in all the circumstances.

28. In the Law Council's view, the requirement that the disclosure is *"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.

29. The Explanatory Memorandum offers no greater insight and unhelpfully provides that the sub-section is

    "..intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure".

30. The Law Council submits that the Bill should be amended to provide greater direction, particularly about the circumstances in which it would not be appropriate to disclose telecommunications data to a foreign law enforcement agency.

31. In that regard, the Law Council submits that the Bill should at least be amended to provide that

    "without limiting sub-section 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."[6]

[6] Proposed subsections 180B(3)(b)(ii) and 180B(8)(b) which relate to the disclosure of prospective telecommunications data also require that the authorising officer consider whether the disclosure is "appropriate in all the circumstances". However, an authorisation can only be issued under these sections in

32. This 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. (Although it is noted that, at least in relation to the AFP, any disclosure would already have to comply with the *AFP Practical Guide on international police-to-police assistance in potential death penalty situations.)*

Seriousness of the Offence

33. Under the current provisions of the TIA Act, an authorised officer within a criminal law-enforcement agency is only able to authorise the disclosure of prospective telecommunications data if the disclosure is reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least 3 years.[7]

34. The proposed provisions of the Bill will similarly provide that, in the context of a foreign investigation, an authorised officer may only authorise the disclosure of prospective telecommunications data where it is reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty.

35. These provisions seek to ensure that prospective telecommunications data may only be obtained and provided to assist in the investigation of a foreign offence if the offence concerned is of a prescribed level of seriousness.

36. However, as above, the Law Council is concerned that under the proposed amendments, the seriousness of the offence being investigated and whether it meets the required threshold test is measured by reference to the maximum penalty imposed for the offence in the requesting country. Such penalties may be considerably out of sync with, and much more severe than, the penalties imposed in Australian jurisdictions for like conduct.

37. The Law Council therefore again submits that the relevant provisions should be amended to require that the offence under investigation would attract the requisite threshold penalty had it been committed in Australia.

38. It should not be possible under the Mutual Assistance Act and 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.

circumstances where the Minister has already received and approved a formal mutual assistance request, having considered the matters set out in section 8 of the Mutual Assistance Act.

[7] *Telecommunications (Interception and Access) Act 1979*, s 180(4)

Privacy Considerations

39. Currently under s180(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."

40. There is no like requirement in the TIA Act to consider privacy impacts when authorising the disclosure of historical telecommunications data.

41. It is proposed in the current Bill to repeal subsection 180(5) and replace it with a new section 180F – see Schedule 2, Part 2, Item 41.

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

43. While the Law Council acknowledges that the insertion of section 180F, a provision of broader application than existing sub-section 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.

44. The Law Council questions the value of a legislative provision which merely requires an authorising officer to "have regard to" privacy impacts.

45. 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.

46. 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.

47. The Law Council raised the same concerns when the current sub-section 180(5) was first introduced into the TIA Act.

48. 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."

49. According to the Explanatory Memorandum, the intent of proposed section 180F 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."

50. The Law Council submits that a test framed in the terms proposed would give greater effect to the purported intent of the section.

Restrictions on use, disclosure, retention and destruction of telecommunications data

51. Proposed section 180E of the TIA Act (see item 41 of Schedule 2) provides that telecommunications data may not be disclosed to a foreign country unless the disclosure is subject to the following conditions:

- 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;
- in the case of information or a document disclosed under section 180B—any other condition determined, in writing, by the Attorney-General.

52. As in relation to the sharing of information about stored communications, the Law Council supports the proposal to impose conditions of this type on the transfer of information. However, as above, the Law Council queries how, in the absence of an undertaking, these conditions would 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.

Conclusion

53. For the reasons outlined above, the Law Council submits that the committee should recommend that the relevant provisions not be enacted or be amended to ensure that before the relevant information is disclosed in the context of foreign investigations, similar matters are considered as those which would be taken into account if it was being disclosed in a domestic context and similar reporting requirements and safeguards for privacy protection are applied. The Law Council notes that it appears that the Cybercrime Convention would not prevent such amendments being made.

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia is the peak national representative body of the Australian legal profession. The Law Council was established in 1933. It is the federal organisation representing approximately 50,000 Australian lawyers, through their representative bar associations and law societies (the "constituent bodies" of the Law Council).

The constituent bodies of the Law Council are, in alphabetical order:

- Australian Capital Territory Bar Association
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society of the Australian Capital Territory
- Law Society of the Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar Association
- The Victorian Bar Inc
- Western Australian Bar Association
- LLFG Limited (a corporation with large law firm members)

The Law Council speaks for the Australian legal profession on the legal aspects of national and international issues, on federal law and on the operation of federal courts and tribunals. It works for the improvement of the law and of the administration of justice.

The Law Council is the most inclusive, on both geographical and professional bases, of all Australian legal professional organisations.