National Interest Analysis [2011] ATNIA 9

with attachment on consultation

Accession by Australia to the Convention on Cybercrime

[2011] ATNIF 5

NATIONAL INTEREST ANALYSIS: CATEGORY 2 TREATY

SUMMARY PAGE

Accession by Australia to the Convention on Cybercrime (Budapest, 23 November 2001) [2011] ATNIF 5

Nature and timing of the proposed treaty action

1. The proposed treaty action is for Australia to accede to the Council of Europe *Convention on Cybercrime* (the Convention), which opened for signature in Budapest on 23 November 2001. The Convention entered into force on 1 July 2004.

2. While Australia is not a member of the Council of Europe and did not participate in the negotiation of the Convention, Article 37(1) provides that the Convention is open to accession by any State which is not a member if they have received an invitation to accede to the Convention. On 20 September 2010, the Council of Europe invited Australia to accede to the Convention.

3. Australia intends to make reservations in relation to Articles 14(3) and 22(2). The Article 14(3) reservation will ensure that foreign investigations must meet existing penalty thresholds in Australian law before certain powers can be exercised. The Article 22(2) reservation relates to the application of State and Territory laws that cannot assert the jurisdiction required by Article 22. Further details are at paras 34-36.

4. Subject to the Joint Standing Committee on Treaties' (JSCOT) recommendation, it is expected that Australia's instrument of accession will be lodged after the enactment of necessary domestic legislative amendments.

5. The Convention will enter into force for Australia on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Overview and national interest summary

6. As the only international treaty on cyber crime, the Convention provides a framework for cyber crime laws and international cooperation. The Convention requires Parties to criminalise certain types of conduct committed via the internet and other computer networks and ensure domestic agencies can access and share information to facilitate international investigations.

7. Accession to the Convention will ensure that Australia can more effectively prevent, detect and prosecute cyber crime offences. Acceding to the Convention will also enhance the ability of Australian domestic law enforcement agencies to collect, share and receive information to assist in domestic and foreign investigations. Currently 30 states are party to the Convention, including one non-member of the Council of Europe – the United States. Seventeen other states have signed the Convention, including three further non-members of the Council of Europe – Canada, Japan and South Africa.

Reasons for Australia to take the proposed treaty action

8. Cyber crime includes criminal activity that targets computers and computer networks (such as unlawful access to computer data or interfering with computer systems) as well as offences where the use of computers or the internet is integral to the offence (such as using the internet for the distribution of child pornography).

9. Globally, cyber crime continues to grow in scale, sophistication and success. As the quantity and value of electronic information has increased, so too have the efforts of criminals and other malicious actors who have embraced the internet as a more anonymous, convenient and profitable way of carrying out their activities.

10. Accession to the Convention will complement Australia's mutual assistance laws, which continue to grow in importance as national boundaries are increasingly spanned by globalised computer networks.

11. Should Australia accede to the Convention, there may be difficulty in assisting agencies from non-Party states with offences or processes inconsistent with the Convention. Australia will need to ensure consistency with the Convention in future policy or reforms to laws relating to access to communications. This may limit autonomy. However, we believe the benefits associated with enhanced international cooperation outweigh these considerations.

Obligations

12. The Convention requires certain conduct to be criminalised, appropriate powers to be available to law enforcement agencies and the introduction of procedures to facilitate information sharing and provide greater multilateral access to information.

Offences

13. The Convention requires Parties to criminalise activity that undermines the confidentiality, integrity and availability of computer data and systems, including:

- unlawful access to a computer system without right;
- illegal interception of communications;
- damaging, deleting, deterioration, alteration or suppression of computer data without right;
- serious hindering of the functioning of a computer system; and
- use of devices designed for the purposes of committing such offences.

14. Parties are also required to establish computer-related and content-related offences aimed at addressing the specific use of technology to commit crime including:

- forgery;
- fraud;
- child pornography; and
- infringements of copyright and related rights.

15. Article 11 requires Parties to establish offences for ancillary liability, such as attempting the commission of such offences. Article 12 requires Parties to ensure that corporate liability applies to the commission of Convention offences. Article 13 requires Parties to ensure the offences are punishable by effective, proportionate and dissuasive sanctions, including imprisonment where appropriate.

16. Article 22 requires Parties to establish jurisdiction over any offence established in accordance with the Convention when the offence is committed:

- in its territory;
- on board a ship flying a flag of that Party;
- on board an aircraft registered under the laws of that Party; or
- by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

17. In addition, Article 22 requires Parties, where appropriate, to consult where more than one Party claims jurisdiction over an offence.

Powers to be conferred upon law enforcement agencies

18. Article 14 requires Parties to provide appropriate powers and procedures for the investigation and prosecution of convention offences, other offences committed by means of a computer system and the collection of electronic evidence. Article 15 requires that all powers and procedures are subject to conditions and safeguards that protect human rights and liberties contained in applicable human rights instruments.

19. Articles 16 to 21 require Parties to enact powers enabling domestic agencies to:

- order or obtain the expeditious preservation of stored computer data (including associated traffic data) for up to 90 days;
- enable the disclosure of associated traffic data to allow the identification of service providers involved in the path of the communication;
- order the production of specific stored computer data, or the production of subscriber information relating to such data held by a service provider;
- search, access, seize and secure a computer, or part of it, or any computer data stored therein;
- collect and record traffic data through technical means on a real-time basis; and
- the interception of communications to investigate certain offences.

20. The convention defines “computer data” as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* and “traffic data” as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Process for exchanging information

21. Articles 23 to 28 contain general obligations relating to international cooperation, including in relation to mutual assistance, extradition and the disclosure of unsolicited information. The obligation to cooperate or provide mutual assistance extends to all criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Article 23 confirms that cooperation is to occur in accordance with existing international agreements on mutual legal assistance and extradition, reciprocal arrangements between Parties and relevant domestic laws.

22. Article 24 deems the offences enumerated in Articles 2-11 of the Convention, where subject to a penalty of one year imprisonment, to be extraditable offences in any extradition treaty between or among the Parties. A Party may also use the provisions of the Convention as a basis for extradition in the absence of an applicable extradition treaty. Article 24(6) also applies the principle 'extradite or prosecute' in respect of these offences. Articles 27 and 28 establish a framework for mutual assistance in circumstances where Parties do not have an existing mutual assistance arrangement, and provide for assurances of confidentiality and restrictions on use.

23. Articles 29 to 34 detail the types of assistance that may be requested between Parties. This assistance includes the preservation of computer data (and associated traffic data) by service providers for both domestic and foreign investigations until an instrument authorising the disclosure is issued, mutual assistance in the disclosure of traffic data in real time and assistance in searching and accessing computer data.

24. Article 29 allows Parties to refuse a request to preserve data in circumstances where the condition of dual criminality cannot be fulfilled in respect of offences other than Convention offences or if the request relates to a political offence, or considers that the execution of the request is likely to prejudice the requested Party's sovereignty, security, public policy or other essential interests.

25. Article 34 provides that mutual assistance regarding the interception of content data is to be provided only to the extent permitted under applicable treaties and domestic law. Australian legislation does not allow for real-time interception by foreign countries. As a result, there will be no obligation to provide this assistance. Article 35 requires Parties to establish a 24 hour, 7 days per week, point of contact to receive requests and provide assistance.

Reservations, Declarations and Final Provisions

26. Article 22(2) allows Parties to reserve the right not to extend the jurisdictional coverage of offences to any Convention offence committed:

- on board a ship flying a flag of that Party;
- on board an aircraft registered under the laws of that Party; or
- by one of its nationals, if the offence is punishable under criminal law in the jurisdiction in which it was committed, or if the offence is committed outside the territorial jurisdiction of any State.

27. Although Commonwealth offences may be able to apply in these circumstances, State and Territory offences will not. Australia intends to avail itself of this reservation in relation to the offences in Articles 7, 8 and 9.

28. Articles 40 and 42 provide for the making of declarations and reservations concerning the Convention. Only reservations listed in Article 42 can be made in relation to the obligations placed on the Parties by the Convention.

29. Reservations must be made in writing at the time of signing or when depositing an instrument of ratification or accession. Article 43 provides that, where a reservation is made, a Party may wholly or partially withdraw it by notification to the Secretary General of the Council of Europe. As explained in paragraphs 34-36, Australia intends to avail itself of the reservations relating to Article 14(3) and Article 22(2).

30. Article 39 provides that the purpose of the Convention is to supplement applicable multilateral or bilateral treaties or arrangements and therefore does not affect other rights, restrictions, obligations or responsibilities of a Party.

31. Article 45 provides that disputes between the Parties regarding the interpretation of the Convention shall be settled through negotiation or other peaceful means agreed by the Parties, including submission to the European Committee on Crime Problems, to an arbitral tribunal for a binding decision or to the International Court of Justice.

Implementation

32. At the time of tabling, Australian law complies with a number of the obligations of the Convention. Australia already has relevant offences in domestic law and the Australian Federal Police provide the necessary 24 hour, 7 days per week, point of contact to deal with international requests for assistance.

33. Accession to the Convention will require amendments to:

- the *Criminal Code Act 1995* to expand the application of the Commonwealth computer offences to meet the Convention obligations;
- the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to enable domestic agencies to preserve and collect traffic data and stored computer data at the request of a foreign country; and
- the *Copyright Act 1968* in order to meet the Convention's extended jurisdiction obligations.

Reservations

34. Australia intends to make two reservations to the Convention. A reservation under Article 14(3) will be required in relation to Article 20 as Australian legislation limits the disclosure of real-time traffic data to investigations relating to a criminal offence punishable by at least three years' imprisonment. Maintaining this threshold will ensure consistency in powers for foreign agencies with existing Australian laws.

35. Disclosing real-time traffic data for a lower threshold would be inconsistent with the TIA Act, which balances the use of covert techniques with the seriousness of offences. Five other States (Bulgaria, Denmark, Finland, Montenegro and Norway) have made reservations under this Article.

36. A reservation is proposed in relation to Article 22(2). Australia intends to comply with Convention obligations through a combination of Commonwealth and State laws. The jurisdiction of State offences cannot be asserted in relation to Article 22(1)(b)-(d). France, Latvia and the United States have made a reservation under this Article.

Costs

37. An increase in requests for the preservation and disclosure of data is likely to result in additional costs for law enforcement, carriers and carriage service providers (C/CSPs). C/CSPs will be able to recover these costs. Generally, under the mutual assistance regime, the costs of providing assistance are borne by the Requested Party. The Australian Federal Police will absorb the costs of additional requests, and additional costs related to the operation of the existing 24/7 Network, as required by Article 35.

Regulation Impact Statement

38. The Office of Best Practice Regulation has been consulted and confirms that a Regulation Impact Statement is not required.

Future treaty action

39. Article 44 provides that amendments to the Convention can be proposed by any Party. Any amendment will then be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Council of Europe Committee of Ministers its opinion on the proposed amendment for consideration. Following consultation with Parties who are not members of the Council of Europe, the Committee may adopt the amendment which will be forwarded to Parties for acceptance. Any amendment shall come into force on the 30th day after all Parties have informed the Secretary General of their acceptance. In other words, unanimous formal acceptance of all Parties is required for any amendment to take effect. Future treaty action, including any amendments to the Convention, would be subject to Australia's domestic treaty process, including consideration by JSCOT.

Withdrawal or denunciation

40. Article 47 provides that any Party may, at any time, denounce the Convention by notification to the Secretary General of the Council of Europe. Any denunciation takes effect on the first day of the month following the expiration of a period of three months after the receipt of the notification by the Secretary General. Withdrawal or denunciation by Australia would be subject to Australia's domestic treaty process, including tabling and consideration by JSCOT.

Contact details

Telecommunications and Surveillance Law Branch
National Security Law and Policy Division
Attorney-General's Department

ATTACHMENT ON CONSULTATION

Accession by Australia to the Convention on Cybercrime (Budapest, 23 November 2001)
[2011] ATNIF 5

CONSULTATION

41. On 17 February, 2011 the Attorney-General's Department released a discussion paper on the Department's website seeking comment on Australia's proposed accession to the Convention. The consultation period is open until 14 March 2011.

42. The discussion paper contains an outline of how cyber crimes are investigated by Australian agencies, the challenges associated with those investigations and how accession to the Convention can assist in addressing some of those challenges.

43. The paper also contains information about the Convention, how Australian laws currently comply with the Convention and areas where amendment would be required to Australian law to enable compliance.

44. The Department also directly advised representatives from State and Territory Governments, law enforcement agencies, the Office of the Privacy Commissioner, the telecommunications industry and other directly affected stakeholders of the public consultation period.

45. The proposed action will have an impact on the State and Territory Governments. Some State and Territory laws that do not currently criminalise activity to facilitate accession will be bound by the proposed amendments to the cyber crime offences in the *Criminal Code Act 1995*. Officers from State and Territory Governments were notified at the Commonwealth State-Territory Standing Committee of Treaties in September 2010 that the Commonwealth Government intended to accede to the Convention.

46. The Government notes that it anticipates that the tabling of the Convention for consideration by JSCOT will occur prior to the conclusion of the consultation period. The Government considers that it is beneficial to advance the accession process as quickly as possible to facilitate the expedited sharing of information to assist both domestic and international investigations of cyber crimes.

47. The Department will inform JSCOT of the outcomes of the public consultation period shortly after its completion on 14 March 2011.