11

Council of Europe Convention on Cybercrime

Introduction

11.1 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.[1] The Council may invite Non-Member States to accede to the Convention. On 20 September 2010 Australia was invited to do so.[2]

11.2 Cybercrime includes 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.[3]

11.3 The *Convention on Cybercrime* is the first international treaty in this area, its main objective being to:

---

1 *National Interest Analysis* [2011] ATNIA 9, Accession by Australia to the Convention on Cybercrime [2011], ATNIF 5, para. 1.

2 Under Council of Europe, Article 37(1), see NIA, para. 2.

3 NIA, para. 8.

> …develop a common criminal policy to combat cyber crime, in particular by adopting appropriate legislation and international co-operation.[4]

11.4 The Convention supplements existing agreements promoting co-operation in the penal field between the Council of Europe and other States, with specific reference to the 1989 *United Nations Convention on the Rights of the Child* and the 1999 *International Labour Organization Worst Forms of Child Labour Convention*.[5]

11.5 The treaty 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.[6]

11.6 To date, over 30 member states and one non-member, the United States, are party to the Convention. Seventeen other nations have signed the Convention, including non-members Canada, Japan and South Africa.[7]

Reasons to support the treaty

11.7 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.[8]

11.8 The Committee notes advice that while Australia currently has specific laws targeting cyber crime—including such offences as unauthorised access, modification or impairment of computers, online child exploitation, copyright infringement and online fraud— law enforcers are

4 *Convention on Cybercrime* (the Convention) Budapest, 23.XI.2001, Not yet in force [2011] ATNIF 5, Preamble.

5 Convention, Preamble.

6 These rights are preserved under various instruments including the 1950 *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms*, the 1966 *United Nations International Covenant on Civil and Political Rights*; and the 1981 *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

7 NIA, para. 7.

8 NIA paras 8 and 9.

increasingly challenged by the transnational and dynamic nature of this type of criminal activity.[9]

11.9 Australia's accession to the Convention will complement existing mutual assistance laws, boosting capacity for international co-operation to deal with increasingly sophisticated and diverse forms of computer-related criminal activity.[10]

11.10 The Attorney-General's Department cited a recent successful operation against child sex abuse to illustrate the effectiveness of international co-operation against this and other areas of cybercrime, such as fraud and terrorism.[11] The Department's representative Mr Geoff McDonald advised:

> Operation Rescue, led to the arrest of nearly 200 suspected paedophiles and rescued 230 children. Operation Rescue commenced as an investigation undertaken by the AFP alone. It then spread to a British investigation. In response, the Federal Police and British police formed a joint investigation, which involved sharing intelligence with police in Thailand and the subsequent discovery of a website publishing child abuse material. It then led to other countries: the Netherlands, the involvement of Europol, Canada, Italy, the United States, New Zealand. People were arrested in Chile, Brazil and France.[12]

11.11 The Uniting Church in Australia, Synod of Victoria and Tasmania, wrote to the Committee in support of Australia's accession to the Convention, with particular regard to the need for greater international effort to combat online child sexual abuse.[13]

11.12 The Church's Justice and International Unit suggests that Australia should utilise international co-operation under the Convention to take down notices for child sex abuse sites, noting that Cambridge University studies

9 Attorney-General's Department, Public Consultation Document: *Australia's Proposed Accession to the Council of Europe Convention on Cybercrime,* 15 February 2011, p. 1.

10 NIA, para. 10.

11 Mr McDonald, Attorney-General's Department, *Transcript of Evidence*, Canberra, 25 March 2011, p. 10.

12 Mr McDonald, Attorney-General's Department, *Transcript of Evidence*, Canberra, 25 March 2011, p. 7.

13 The submission cited findings that both commercial and non-commercial child sex abuse domains are widespread, with commercial child sex materials being accessed by two million people globally and peer to peer non- commercial networks generating an estimated 50 000 new child sex images each year. Ref. United Nations' report *The Globalisation of Crime: a Transnational Organised Crime Threat Assessment (*17 June 2010), in the Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 2*, p. 2.

have found that sites threatening commercial bank interests are taken down very quickly by comparison.[14]

11.13 The *National Interest Analysis* (NIA) to the treaty advised that to vitalise this international co-operation Australia must accept some loss of autonomy, as future policy and law reform should be consistent with that mandated under the Convention. Conversely, failure to accede to the Convention will diminish Australia's capacity to assist non-party states combat offences or processes inconsistent with it, to the detriment of international law enforcement in this area.[15]

11.14 The Attorney General's representatives emphasised in conclusion that Australia should not under estimate the strategic importance of acceding to the Convention, which has elicited strong support among the international community.[16]

11.15 The Committee notes that the thirty nations which have ratified or acceded to the Convention, and further 17 which are signatories with intention to ratify it, comprise many major treaty allies with Australia.[17]

Obligations

11.16 The Convention requires countries to criminalise offences related to computer systems and data, with a view to harmonising domestic criminal laws and reducing barriers to international co-operation.[18]

11.17 The Convention (Chapter 2, Section 1) provides for national level obligations under four titles, covering:

- Title 1— 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;[19]

14 T Moore and R Clayton, 'The Impact of Incentives on Notice and Take–down', Computer Laboratory, University of Cambridge, 2008 <http://www.cl.cam.ac.uk/~rnc1/takedown.pdf> viewed 21 March 2011.

15 NIA, para. 11.

16 Mr Geoff McDonald, Attorney-General's Department, *Transcript of Evidence*, Canberra, 25 March 2011, p. 14.

17 Ms Catherine Smith, Attorney-General's Department, *Transcript of Evidence*, Canberra, 25 March 2011, p. 13.

18 Convention Preamble.

19 Articles 1 to 6.

- Title 2—computer-related offences, including forgery and fraud;[20]
- Title 3—content-related offences, including child pornography;[21] and
- Title 4—offences related to infringements of copyrights and related rights.[22]

11.18 Title 5, Articles 11 to 13 respectively, require Parties to: establish offences for ancillary liability, such as attempting the commission of such offences; ensure that corporate liability applies to the commission of Convention offences; and, that offences are punishable by effective, proportionate and dissuasive sanctions, including imprisonment where appropriate.[23]

11.19 Section 2 of the Agreement covers the fundamentals of Procedural law, in particular:

- Article 14—requires parties to establish necessary powers and procedures to investigate and prosecute convention offences; and
- Article 15—determines that these powers must be subject to conditions and safeguards contained in applicable human rights instruments.

11.20 Procedures to facilitate international crime co-operation and make investigations more efficient under the Convention are at Articles 16 to 21, and enable 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
- intercept of communications to investigate specified offences.[24]

20 Articles 7 and 8.
21 Article 9.
22 Article 10.
23 NIA, para. 15.
24 NIA para. 19.

11.21 In Section 3, covering Jurisdiction, Article 22 (2) allows parties the right not to extend jurisdictional coverage of offences in certain circumstances.

11.22 According to the NIA for the Convention, Australia intends to make a Reservation to Article 22 (2), in relation to prosecution under Articles 7, 8 and 9 (computer related forgery, computer related fraud, and offences related to child pornography) which is effected under Commonwealth not State and Territory law.[25]

11.23 Chapter 3, Articles 23 to 28 cover general obligations for international co-operation. Article 24 deems Convention Offences, where subject to a penalty of one year imprisonment, are extraditable offences in any extradition treaty between or among the Parties.

11.24 Articles 27 and 28, respectively, 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 of information obtained under those circumstances.

11.25 Articles 29 to 34 detail the types of assistance that may be requested between Parties including:

- 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**,** parties may also refuse a request to preserve data in circumstances where the condition of dual criminality cannot be fulfilled;[26]
- mutual assistance in the disclosure of traffic data in real time, but only to the extent permitted under applicable treaties and domestic law (Australian legislation does not allow for real-time interception by foreign countries);[27] and
- establishment of a 24 hour, 7 days per week (24/7) point of contact to receive requests and provide assistance for searching and accessing computer data.[28]

25 NIA paras 27, 36.
26 Article 29.
27 Article 34.
28 Article 35.

Implementation

11.26 The Convention requires that parties have appropriate domestic laws in place for criminal enforcement and interception of cybercrime. The Committee was advised that Australia is largely prepared, as domestic law has been progressively reformed to support the Convention. In particular reforms were made to the *Criminal Code Act 1995* in 2000 to address cybercrime offences.[29]

11.27 Accession to the Convention will require further amendments to:

- the *Criminal Code Act 1995* (the Criminal Code) 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.[30]

11.28 The NIA notes that Australia otherwise has capacity to meet international obligations for enforcement, such as in provision of the necessary 24/7 contact point to respond to international requests for assistance through the Australian Federal Police.[31]

Concerns about the Convention

11.29 As set out above, Australia's accession to the *Convention on Cybercrime* will require some immediate amendment to existing legislation, and the loss of a degree of autonomy in future domestic law reform to preserve agreement with treaty obligations.[32]

11.30 A number of concerns were raised in evidence about the potential impact of ratification of this Convention on the integrity of Australia's regulation of computer communications, both in respect of individual rights and

29 Mr McDonald, Attorney-General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, p. 9.

30 NIA, para.

31 NIA, para. 32.

32 NIA, para. 11.

privacy protections and on the capacity of the States and Territories to retain and implement relevant enforcement powers within their jurisdictions.

Privacy and the preservation of data

11.31 The Committee received submissions maintaining that the Convention does not contain sufficiently robust privacy and civil liberties protections to offset the increased surveillance and information sharing powers it implements. Of particular concern were powers governing the real-time collection and preservation of computer data.[33]

11.32 Attorney-General's Department representative Ms Catherine Smith advised that the capacity to access and preserve data is fundamental to the new mutual assistance arrangements:

> Currently telecommunications providers delete text messages or emails after a very short period of time and so the convention has a prevention of the deletion of that information where there is to be a warrant served upon them. It is preserving that data to allow time for mutual assistance requests to go through or, in domestic cases, for the police to obtain a warrant.[34]

11.33 The Department also advised that there is no domestic law supporting this obligation, so current interception legislation must be amended to support this requirement.[35]

11.34 As discussed in more detail below, submissions from the Law Council of Australia and the Pirate Party Australia maintained that there has not been sufficient transparency about the Convention's obligations and procedures to determine whether any necessary legislative amendments will be consistent with Australia's existing privacy regime.[36]

11.35 The Pirate Party Australia, a civil liberties advocacy organisation, had particular concerns about arrangements for mass surveillance and data retention under the Convention:

> We agree with the proposition that law enforcement require[s] a coordinating mechanism to enable those agencies to tackle online

33 Articles 20 and 21.

34 Attorney–General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, p. 10.

35 In particular to issue authentication certificates requiring data to be preserved in accordance with domestic or international mutual assistance requests. Ms Smith Attorney–General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, pp. 10–11.

36 Law Council of Australia, *Submission 3*, p. 2 and Pirate Party Australia, *Submission 4*, p. 3.

> criminal elements globally, however we should be very mindful that these mechanisms do not throw fundamental freedoms and respect for individual rights and democratic institutions to the wind. We do not accept that combating cybercrime must lead to erosion of fundamental protections of privacy and the protection of personal data.[37]

11.36 Department representatives, however, maintained that these concerns are out of proportion to the actual requirements imposed by the Convention.

11.37 Mr McDonald and Ms Smith dispelled concerns about threats to privacy on accessing of the data content of stand-alone computers, noting that warrants would be required and that networked activity would be the principal means of surveillance for detection and enforcement.[38]

11.38 Ms Smith addressed questions about real-time surveillance, emphasising that powers for mass surveillance activities, such as wire tapping or eavesdropping,[39] are not enhanced under the Convention as the amendments are limited to telecommunications legislation not Commonwealth or State surveillance device legislation.[40]

11.39 Additionally, she advised, Australia would lodge a Reservation to requirements for foreign investigation of real-time data (under Article 14 (3)) to ensure they matched Australian thresholds.[41] In particular, Australian law limits disclosure of real-time traffic data to investigations relating to a criminal offence punishable by at least three years' imprisonment.[42]

11.40 In relation to broader concerns about the lack of appropriate civil liberties protections under the Convention,[43] the Committee referred to Convention Article 15, which specifically requires powers and procedures to be exercised in accordance with relevant international human rights instruments. Article 15 (3) also provides that matters be subject to judicial or other supervision:

---

37 Pirate Party Australia, *Submission 4*, p. 2.

38 Attorney–General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, pp. 9, 10. Australia Patriot Movement, *Submission 1.1*, also raised issues about stand-alone computers.

39 Pirate Party Australia, *Submission 4*, p. 3.

40 Attorney–General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, pp. 11, 15, and see NIA para. 34.

41 Ms Smith, Attorney–General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, pp. 11, 15.

42 NIA paras 25 and 34.

43 Pirate Party Australia, *Submission 4*, p. 2.

> To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

11.41 The Committee also acknowledges Departmental advice that further changes to the *Mutual Assistance in Criminal Matters Act 1987*, the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Copyright Act 1968* would be constrained by the constitutional underpinnings of these established Acts, which have strong privacy safeguards and accountability mechanisms.[44]

Jurisdiction issues

11.42 The NIA to the Convention notes that ratification of the treaty may have an impact on the State and Territory Governments, as some State and Territory laws do not currently criminalise activity but will be bound by the proposed amendments to the cyber crime offences in the Criminal Code.[45]

11.43 Jurisdiction issues are covered in Article 22 (2) which requires that each Party is to 'adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established' for the purposes of the Convention.

11.44 As noted, Australia will lodge a Reservation to the Convention with reference to Article 22 (2) to allow for compliance with these obligations under a combination of Commonwealth and State and Territory laws.[46]

11.45 The Committee investigated jurisdictional issues raised in relation to the Reservation by the Government of Western Australia. In its submission, the West Australian Government asserted it had extra-territorial legislative competence to make constitutionally valid laws to support the Convention and wanted to be consulted about the drafting of the reservation, and any changes which might affect the State's powers in that regard.[47]

---

44 Mr McDonald and Ms Smith, Attorney-General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, pp. 9, 13.

45 NIA Consultation, para. 45.

46 NIA, para. 36.

47 Government of Western Australia, *Submission 5*, p. [1].

11.46 In particular, the submission stated:

> It is important to note that accession to the Convention should not create further bureaucracy which could act to stifle established links between agencies, particularly those formed at a State level. WA Police already has strong ties with a number of overseas policing agencies and a number of service providers in attempting to tackle cybercrime. It would be detrimental if accession to the Convention were to erode these links.[48]

11.47 The Attorney-General's Department undertook to answer Questions on Notice in relation to this matter. It advised that no extra level of bureaucracy would be entailed under the Convention as all requests for international information will continued to be channelled through the Federal Police's 24/7 response centre.[49]

11.48 The Department also stated that the proposed reservation under Article 22 (2) will address technical issues only, but is necessary to allow for States and Territories to regulate offence obligations, such as for computer related forgery and fraud under Convention articles 7 and 8. Consultation will be undertaken with States and Territories if an impact on their laws is indicated.[50]

11.49 The Attorney General also committed to write to all States and Territories in response to this and other concerns raised in submissions received during recent public consultation on the Convention.[51] In a subsequent supplementary submission on this issue, the Attorney General provided advice received from the Queensland and the Victorian Attorneys-General.[52]

11.50 The Committee notes that the Victorian Attorney General, the Hon. Robert Clark MP, did not support accession to the Convention at this time, due to concerns that State laws may be invalidated under the Commonwealth Criminal Code and Convention obligations, pending outcomes on cases currently before the High Court.[53]

---

48 Government of Western Australia, *Submission 5*, p. [1].

49 Attorney-General's Department, *Submission 6,* Response to Question on Notice 3.

50 Ms Smith, Attorney-General's Department, *Transcript of Evidence,* Canberra, 25 March 2011, p. 15, and Attorney-General's Department, *Submission 6,* Response to Question on Notice 4.

51 Attorney-General's Department, *Submission 6,* Response to Question on Notice 2.

52 Attorney-General's Department, *Submission 6. 1.*

53 viz: *Dickson v The Queen* [210] HCA 30; 9210) 270 ALR1, attachment to Attorney-General's Department, *Submission 6. 1.*

11.51 In response, the Commonwealth Attorney General advised that Convention obligations would be substantially met under existing Commonwealth laws, although an amendment to Part 10. 7 of the Criminal Code—to remove current requirements for offending to involve use of a carriage service, Commonwealth computer or data—would be necessary to close gaps in State and Territory laws.

11.52 The Attorney General observed that this incremental expansion of the Commonwealth offences to fully implement the Convention's obligations would not, however, have a substantive effect on State and Territory offences, given:

> Part 10.7 of the Criminal Code contains a savings clause that explicitly provides that the commonwealth computer offences are not intended to limit or exclude the operation of any law of a State or Territory. This savings clause will continue to apply.[54]

Concerns about the review process

11.53 Prior to the tabling of the Convention on Cybercrime in Parliament, the Attorney General the Hon. Robert McClelland MP issued a consultation paper on Australia's accession to the Convention on 18 February 2011, asking for comment by 14 March 2011.[55]

11.54 The document, entitled *Australia's Proposed Accession to the Council of Europe Convention on Cybercrime* (15 February 2011), provided an introduction and background to the Convention and the treaty process, an outline of obligations (along the lines of that set out in the NIA for the treaty) and some reasons to support the accession.[56]

11.55 On 21 February 2011 the Attorney General wrote to the Committee's Chairman stating that he believed it would be in the national interest that enabling legislation for the treaty be introduced during the Autumn sittings, and before the Committee had an opportunity to review the Treaty. The Treaty was tabled on 1 March 2011.

54 Attorney-Generals' Department, *Submission 6. 1.*

55 Attorney General and Minister for Home Affairs and Justice the Hon Brendan O'Connor, 'Public Consultation on International Convention on Cybercrime', *Joint Media Release,* 18 February 2011.

56 Attorney–General's Department, Proposed Accession to the Council of Europe *Convention on Cybercrime* <http://www.ema.gov.au/www/agd/agd.nsf/Page/ Consultationsreforms andreviews_ProposedAccessiontotheCouncilofEuropeConventiononCybercrime>viewed at 14 April 2011.

11.56 The Law Council of Australia was critical of the fact that the Committee's inquiry process overlapped with the Attorney-General Department's consultation on the Convention. It considered the overall inquiry time insufficient overall and notes that lack of detail on proposed legislative changes to support the Convention may result in changes being introduced as a *fait accompli*, without proper scrutiny.[57]

11.57 The Committee notes that a draft of the treaty was initially released in 2000, and well in advance of Australia announcing its intention to sign the Convention in May 2010.[58]

11.58 However, the Pirate Party of Australia criticised the drafting and formulation of the Convention which it considered was 'opaque and undemocratic', maintaining:

> Even after the release of the draft, and with public consultation, very little substantive change was made to the document and there has been very little in way of acknowledgement to the concerns of privacy and human rights organisations. To submit to a treaty, the draft of which was conducted with such disregard for the democratic and participatory process, condones this process of lawmaking.[59]

Conclusion

11.59 The Committee recognises that cybercrime constitutes a growing threat in a century where computer-based networks have become the most vital and innovative means of communicating and doing business.

11.60 The global and dynamic nature of the medium necessitates a commensurate need for more sophisticated networks of communication and co-operation between nations to regulate the growth and diversification of criminal activity in cyberspace.

11.61 The Committee is also aware that the surveillance of computer-based communications and data storage by law enforcers raises fears about the invasion of privacy, with potential threat to human rights and civil liberties.

---

57 *Submission 3*, pp. 1–2.

58 'Australia to Sign Cyber Treaty', *ITNews for Australian Business* <http://www.itnews.com.au/News/173461, australia-to-sign-international-cybercrime-treaty.aspx> viewed 12 April 2011.

59 *Submission 4*, p. 5.

11.62 The Convention itself does, however, contain guarantees for human rights protection and judicial review, and there is reason to be confident that these protections will be enforced: the framework of domestic law effected by Australia's accession to the Council of Europe *Convention on Cybercrime* provides robust privacy safeguards and accountability mechanisms.

11.63 Notwithstanding these assurances, 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.

11.64 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.

Recommendation 13

The Committee supports Australia's accession to the Council of Europe *Convention on Cybercrime* and recommends binding treaty action be taken.

Recommendation 14

The Committee recommends that the Attorney General report to the Committee on any proposed amendments to Commonwealth or State and Territory law in support of the Council of Europe *Convention on Cybercrime*.

Kelvin Thomson MP

Chair