

Communications Alliance
&
Australian Mobile Telecommunications Association (AMTA)

Response
to the
Attorney-General's Department
Public Consultation
on
Australia's proposed accession to the
Council of Europe Convention on Cybercrime

14th March 2011

INTRODUCTION

- 1 Communications Alliance is the peak telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups. Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see <http://www.commsalliance.com.au>.
- 2 The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. AMTA's mission is to promote an environmentally, socially and economically responsible and successful mobile telecommunications industry in Australia. AMTA members include mobile Carriage Service Providers, handset manufacturers, retail outlets, network equipment suppliers and other suppliers to the industry. For more details about AMTA, see <http://www.amta.org.au>.
- 3 Communications Alliance and AMTA (the Associations) welcome the opportunity to respond to the Attorney-General's Department's (AGD) public consultation paper (Consultation Paper) on Australia's proposed accession to the Council of Europe Convention on Cybercrime (Convention). Members of the Associations may choose to make individual submissions.

INDUSTRY POSITION

- 4 The Associations recognise the policy drivers for the proposed accession and have no fundamental concerns. The comments following are focussed on potential areas of concern to the telecommunications industry should there be consequential changes arising to their legislated obligations under the Telecommunications Interception and Access Act 1979 (TIA Act) and the Telecommunications Act 1997 (Telco Act) and any amendments. The Associations regard the investigation powers required under the Convention, to the largest part, as cyber-specific equivalents of traditional investigation measures existing in the above legislation. To the extent that the "Outline of the articles of the Council of Europe Convention on Cybercrime and Australia's compliance" public consultation document produced by the Attorney-General's Department indicates compliance in any area the Associations rely upon this indication such that there will be no change to current law as a result of the proposed accession.
- 5 The Associations note the possibility of adopting a 'fast freeze, quick thaw' preservation procedure of data that is already in a carrier and/or carriage service provider's (C/CSP) possession to ensure the availability of traffic data in relation to specific criminal investigations (as opposed to a routine, blanket data preservation scheme).
- 6 Moreover, industry positively notes the explicit limitation of Articles 20 and 21 of the Convention to collect and record real-time traffic and content data "within [the C/CSP's] existing technical capability"¹.
- 7 To the extent that amendments to existing Australian law are required, particularly with regards to (but without limitation to) an expedited preservation of data and a preservation period of 90 days (Article 16 of the Convention), the Associations trust that industry will be given sufficient opportunity to provide input to this legislative

¹ ETS 185 – Convention on Cybercrime, 23.XI.2001, Article 20(1b) and Article 21(1b)

process in due time.

- 8 Potential direct consequences of accession are an increased volume of requests (now including requests from international agencies) and the 24/7 availability of a contact point (Article 35 of the Convention). This increased volume may necessitate substantial changes to current operational procedures and resourcing at an industry level. Further, to the extent the 24/7 contact point is passed on to the C/CSP level, this will also affect procedures and resourcing. Industry will review existing cost recovery arrangements to adequately reflect the additional burden imposed.
- 9 In relation to proposed amendments to the preservation regime, the Associations would like to highlight the need for reciprocal mandatory lead in times where implementation of the new obligations imply changes to systems and processes on behalf of the C/CSP. The Associations are willing to work with the Agencies to see these reflected.
- 10 Furthermore, in the absence of any indication to the contrary the Associations assume that an accession to the Convention would not place any obligations on C/CSPs to investigate whether or not corresponding overseas privacy laws are in place prior to handing over any requested information, nor any requirement to ensure that the conditions of disclosure of any particular information have been met by the overseas requestors. The Associations assume that this burden would fall upon law enforcement to ensure that a serious crime was involved in the request or other conditions as specified by current legislation.

ISSUES FOR FUTURE CONSIDERATION / RECOMMENDATIONS

- 11 The Associations consider that it is timely and appropriate to highlight issues for future consideration, as set out below.
- 12 In any legislative changes arising from the accession to the Convention, a harmonisation of language/terms might be appropriate. Specifically, it is noted that:
 - a. the term 'traffic data' (as well as the entire Convention) relate to communications over a computer system and it is not clear to what extent telecommunications systems are meant to be included.
 - b. neither 'telecommunications data' nor 'traffic data' are defined in the TIA Act or the Telco Act. Accordingly, there may be a need to develop a definition of 'traffic data' in line with the term 'telecommunications data' as used but not defined in the TIA Act to ensure consistency between the Convention, the TIA Act and the Telco Act.
 - c. the lack of specificity in the definitions contained in the Convention do not make it clear to what extent telecommunications network equipment forms part of a 'computer system'. The Associations express their concern that this lack of specificity must not imply an extension of the powers given to agencies to include the ability to seize and remove or interfere with telecommunications network equipment/elements/databases including traffic data. Such items may be vital to the operation of the network and any seizure and removal would have the potential to severely affect large numbers of customers. Industry's view is that the current legislation provides sufficient powers for Agencies to access information held by C/CSPs.
 - d. The Associations also point out that there appears to be no link between a 'computer system' and a 'telecommunications system' in the Australian telecommunications law.

- 13 The processes and standards of data exchange with foreign agencies/authorities are unclear at this point in time and would require further elaboration and consultation.
- 14 Industry seeks clarification whether the frequently used practice of supplying Evidentiary Certificates to provide 'authenticity' of the information requested under warrant (in lieu of an appearance in court as a witness) could be used in other jurisdictions. If this is not the case, would there be a need for evidence from industry staff and, if so, through what process would any costs associated with the provision of evidence (e.g. overseas court appearance) be reimbursed?
- 15 As a more general note the Associations highlight that any amendments to the Privacy Act 1988, Telco Act or TIA Act that place any additional obligations on C/CSPs regarding the disclosure of communications content or customer data, both to Australian authorities and overseas, ought to embody the principles included in the Convention of being "effective, proportionate and dissuasive."²

² ETS 185 – *Convention on Cybercrime, 23.XI.2001, Article 13*