

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.

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
CANBERRA



European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

(Budapest, 23.XI.2001)

Not yet in force
[2011] ATNIF 5

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in 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 other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, **No. R (87) 15** regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

- a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b "computer data" means 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;
- c "service provider" means:
 - i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
 - ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;
- d "traffic data" means 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.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
 - a the production, sale, procurement for use, import, distribution or otherwise making available of:
 - i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
 - b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

*Title 2 – Computer-related offences***Article 7 – Computer-related forgery**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a any input, alteration, deletion or suppression of computer data;
- b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

*Title 3 – Content-related offences***Article 9 – Offences related to child pornography**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a producing child pornography for the purpose of its distribution through a computer system;
 - b offering or making available child pornography through a computer system;
 - c distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - e possessing child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
 - a a minor engaged in sexually explicit conduct;
 - b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

- 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
- a a power of representation of the legal person;
 - b an authority to take decisions on behalf of the legal person;
 - c an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
 - b other criminal offences committed by means of a computer system; and
 - c the collection of evidence in electronic form of a criminal offence.
- 3
- a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
 - b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
 - i is being operated for the benefit of a closed group of users, and
 - ii does not employ public communications networks and is not connected with another computer system, whether public or private,that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under 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 other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
- 3 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.

*Title 2 – Expedited preservation of stored computer data***Article 16 – Expedited preservation of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
 - a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
 - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

*Title 3 – Production order***Article 18 – Production order**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
 - a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

- b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
- a the type of communication service used, the technical provisions taken thereto and the period of service;
 - b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
 - c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
- a a computer system or part of it and computer data stored therein; and
 - b a computer-data storage medium in which computer data may be stored
- in its territory.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - b make and retain a copy of those computer data;

- c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
- a collect or record through the application of technical means on the territory of that Party, and
 - b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party; or
 - ii to co-operate and assist the competent authorities in the collection or recording of,
- traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

- 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

- a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party, or
 - ii to co-operate and assist the competent authorities in the collection or recording of,
content data, in real-time, of specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - a in its territory; or
 - b on board a ship flying the flag of that Party; or
 - c on board an aircraft registered under the laws of that Party; or
 - d 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.
- 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it

does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

- 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
- 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

- 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
 - b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
- 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
- 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

- 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
- 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
- b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

- 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
- 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
- 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
- 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual

criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

- 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
- 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

- 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2
 - a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
 - b The central authorities shall communicate directly with each other;
 - c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
 - d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

- 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
- 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
 - a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

- 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not

apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

- 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
 - a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
 - b not used for investigations or proceedings other than those stated in the request.
- 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
- 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

- 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
- 2 A request for preservation made under paragraph 1 shall specify:
 - a the authority seeking the preservation;
 - b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
 - c the stored computer data to be preserved and its relationship to the offence;
 - d any available information identifying the custodian of the stored computer data or the location of the computer system;
 - e the necessity of the preservation; and
 - f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
- 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

- 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
- 5 In addition, a request for preservation may only be refused if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
 - b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

- 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
- 2 Disclosure of traffic data under paragraph 1 may only be withheld if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

- 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

- 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
- 3 The request shall be responded to on an expedited basis where:
 - a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

- 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
- 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

- 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or,

if permitted by its domestic law and practice, directly carrying out the following measures:

- a the provision of technical advice;

- b the preservation of data pursuant to Articles 29 and 30;
 - c the collection of evidence, the provision of legal information, and locating of suspects.
- 2
- a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
 - b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
- 3
- Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

- 1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
- 2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
- 3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
- 4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

- 1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
- 2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force 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.

Article 38 – Territorial application

- 1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
- 2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
- 3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

- 1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
 - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
 - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
 - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
- 2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
- 3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

- 1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
- 2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
- 3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

- 1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
- 2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
- 3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

- 1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
- 2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
- 3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
- 4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
- 5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

- 1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
- 2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

- 1 The Parties shall, as appropriate, consult periodically with a view to facilitating:
 - a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
 - b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
 - c consideration of possible supplementation or amendment of the Convention.
- 2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

- 3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
- 4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
- 5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

- 1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
- 2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d any declaration made under Article 40 or reservation made in accordance with Article 42;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to

the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.