An Advocacy Handbook for the Non Governmental Organisations

The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems

First Published: December 2003
(Updated and revised in May 2008)

Dr. Yaman AKDENIZ, Senior Lecturer in Law, School of Law, University of Leeds, United Kingdom. Director, Cyber-Rights & Cyber-Liberties (UK), and a 2003 Fellow of the International Policy and Information Policy Fellowship programmes of the Open Society Institute. E-mail: lawya@cyber-rights.org

Acknowledgements
This publication was made possible by a grant from the Open Society Institute Information Policy Programme (http://www.soros.org/initiatives/information).

restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested. If You create a Derivative Work, upon notice from any Licensor You must, to the extent practicable, remove from the Derivative Work any reference to such Licensor or the Original Author, as requested.

You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Derivative Works or Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; in the case of a Derivative Work, a credit identifying the use of the Work in the Derivative Work (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Derivative Work or Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer

By offering the Work for public release under this License, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

Licensor has secured all rights in the Work necessary to grant the license rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory license fees, residuals or any other payments;

The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

EXCEPT AS EXPRESSLY STATED IN THIS LICENSE OR OTHERWISE AGREED IN WRITING OR REQUIRED BY APPLICABLE LAW, THE WORK IS LICENSED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING THE CONTENTS OR ACCURACY OF THE WORK.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, AND EXCEPT FOR DAMAGES ARISING FROM LIABILITY TO A THIRD PARTY RESULTING FROM BREACH OF THE WARRANTIES IN SECTION 5, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Derivative Works or Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

Each time You distribute or publicly digitally perform a Derivative Work, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

Executive Summary

The Cyber-Crime Convention 2001 and its Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems have been developed by the Council of Europe, an international and well respected organisation with a primary mission to strengthen democracy, human rights, and the rule of law throughout its member states. Although the Cyber-Crime Convention states in the preamble that a proper balance needs to be ensured between the interests of law enforcement and respect for fundamental human rights, the balance resolutely and regrettably favours the former.

While the CoE's concerns in relation to cyber-crimes and its desire to address criminal law and mutual assistance in criminal matters are shared by many, any co-ordinated policy initiative at an international level should ideally aim to offer the best protection for individual rights and liberties. Lamentably, this has not been the case.

This advocacy handbook for the NGOs provides a policy analysis of the Cyber-Crime Convention 2001 and the Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems from a human rights perspective for policy specialists, NGOs, and human rights activists within the 45 member states of the Council of Europe. Compatibility problems with the European Convention on Human Rights and implications for freedom of expression, privacy of communications and data protection will be the main focus of this critical analysis. The appendices include other useful information that could be relied upon while NGOs and policy activists lobby their individual governments in relation to the implementation of the Cyber-Crime Convention and the first additional protocol.

Introduction

The Cyber-Crime Convention has been developed by an international and well respected organisation with a primary mission to strengthen democracy, human rights, and the rule of law throughout its member states. Although the Cyber-Crime Convention states in the preamble that a proper balance needs to be ensured between the interests of law enforcement and respect for fundamental human rights, the balance resolutely and regrettably favours the former.

While the CoE's concerns in relation to cyber-crimes and its desire to address criminal law and mutual assistance in criminal matters are shared by many, any co-ordinated policy initiative at an international level should ideally aim to offer the best protection for individual rights and liberties. Lamentably, this has not been the case.

The signing and ratification process for both the Convention and the Additional Protocol resulted with 39 member states (plus the external supporters United States, Canada, South Africa, Japan, and Montenegro) signing and 22 countries (Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine, and United States of America) ratifying the main convention as of May 2008 out of the potential 50 countries (45 CoE member states plus the above mentioned external supporters). Following the first five ratifications, the Cyber-Crime Convention came into force on 01 July, 2004. On the other hand 32 member states (including the external supporter Canada, Montenegro, and South Africa) have signed the additional protocol since it was opened to signature in January 2003, and 12 member states (Albania, Armenia, Bosnia and Herzegovina, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia) have ratified the Additional Protocol as of May 2008. Following the initial five ratifications the Additional Protocol came into force on 01 March, 2006.

The next phase of action will lie at the national level where the member states of the Council of Europe will consider signing and ratifying both the Cyber-Crime Convention and the Additional Protocol

concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems. Consequently, in terms of NGOs and civil society representatives, urgent action at the local level is needed. This can only take place once there is wide awareness and knowledge about the serious implications of the work of the Council of Europe in this field. Specifically, a critical assessment of the Cyber-Crime Convention and the additional protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems is necessary.

Objective & Target Audience

This advocacy handbook for the NGOs will provide a policy analysis of the Cyber-Crime Convention 2001 and its first additional protocol from a human rights perspective for policy specialists, NGOs, and human rights activists within the 45 member states of the Council of Europe. Compatibility problems with the European Convention on Human Rights and implications for freedom of expression, privacy of communications and data protection will be the main focus of this critical analysis. The appendices will include other useful information that could be relied upon while NGOs and policy activists lobby their individual governments in relation to the implementation of the Cyber-Crime Convention and the first additional protocol.

Introduction to the Council of Europe

The Council of Europe is an intergovernmental organisation which aims:

- to protect human rights, pluralist democracy and the rule of law;
- to promote awareness and encourage the development of Europe's cultural identity and diversity;
- to seek solutions to problems facing European society (discrimination against minorities, xenophobia, intolerance, environmental protection, human cloning, Aids, drugs, organised crime, etc.);
- to help consolidate democratic stability in Europe by backing political, legislative and constitutional reform.

The Council of Europe covers all major issues facing European society other than defence, and has 45 member states:

Albania (13.07.1995), **Andorra** (10.11.1994), **Armenia** (25.01.2001), **Austria** (16.04.1956), **Azerbaijan** (25.01.2001), **Belgium** (05.05.1949), **Bosnia & Herzegovina** (24.04.2002), **Bulgaria** (07.05.1992), **Croatia** (06.11.1996), **Cyprus** (24.05.1961), **Czech Republic** (30.06.1993), **Denmark** (05.05.1949), **Estonia** (14.05.1993), **Finland** (05.05.1989), **France** (05.05.1949), **Georgia** (27.04.1999), **Germany** (13.07.1950), **Greece** (09.08.1949), **Hungary** (06.11.1990), **Iceland** (09.03.1950), **Ireland** (05.05.1949), **Italy** (05.05.1949), **Latvia** (10.02.1995), **Liechtenstein** (23.11.1978), **Lithuania** (14.05.1993), **Luxembourg** (05.05.1949), **Malta** (29.04.1965), **Moldova** (13.07.1995), **Netherlands** (05.05.1949), **Norway** (05.05.1949), **Poland** (29.11.1991), **Portugal** (22.09.1976), **Romania** (07.10.1993), **Russian Federation** (28.02.1996), **San Marino** (16.11.1988), **Serbia and Montenegro** (03.04.2003), **Slovakia** (30.06.1993), **Slovenia** (14.05.1993), **Spain** (24.11.1977), **Sweden** (05.05.1949), **Switzerland** (06.05.1963), "**The former Yugoslav Republic, of Macedonia**" (09.11.1995), **Turkey** (09.08.1949), **Ukraine** (09.11.1995), **United Kingdom** (05.05.1949)[1]

[1] The Council of Europe map is taken from http://www.coe.int/T/E/Com/About_Coe/Member_states/default.asp

There are also some states which were granted observer status and these are:
Canada (29.05.1996) - **Holy See** (07.03.1970) - **Japan** (20.11.1996) - **Mexico** (01.12.1999) - **United States of America** (10.01.1996) – to the Committee of Ministers; and, **Canada** (28.05.1997) - **Israel** (02.12.1957) - **Mexico** (04.11.1999) - to the Parliamentary Assembly

The Council of Europe's most significant achievement is the European Convention on Human Rights, an international treaty which was adopted in 1950 and came into force in 1953. It sets out a list of rights and freedoms which states are under an obligation to guarantee to everyone within their jurisdiction. It has also established international enforcement machinery whereby states and individuals, regardless of their nationality, may refer alleged violations by contracting states of the rights guaranteed in the Convention to the judicial institutions in Strasbourg established by the Convention. Another significant achievement by the Council of Europe is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[2] ("Data Protection Convention") which was adopted in January 1981.[3] The Data Protection Convention was the first legally binding international instrument in the data protection field.

History of the Cyber-Crime Convention and the Additional Protocol

The Council of Europe ("CoE") Cyber-Crime Convention 2001 is the first international treaty to address criminal law and procedural aspects of various types of offending behaviour directed against computer systems, networks or data in addition to content related crimes such as child pornography. In general the Convention aims to harmonise national legislation in this field, facilitate investigations and allow efficient levels of co-operation between the authorities of different member states of the CoE and other third party states who would be party to the Convention following a ratification process at the national level.[4] The development of the Convention certainly follows from the previous work of the CoE in relation to computer-related crimes,[5] but also expands upon the previous work conducted and would be binding on signing states when the ratification process is completed at the national level.

---

2 ETS No. 108, Strasbourg, 28 January, 1981.

3 See generally http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/ in relation to the Data Protection related activities of the Council of Europe.

4 The text of the draft Convention can be found at http://conventions.coe.int/treaty/en/projects/cybercrime.htm

5 Council of Europe Committee of Ministers, Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies), at http://cm.coe.int/ta/rec/1989/89r9.htm, Council of Europe Committee of Ministers, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies), at http://cm.coe.int/ta/rec/1995/95r13.htm

A Committee of Experts on Crime in Cyberspace ("PC-CY") was established within the Council of Europe to draw up the Cyber-Crime Convention[6] to fight *inter alia* substantive offences committed through the use of the Internet in 1997.[7] A number of non member states such as the US, Canada, Japan, and South Africa also contributed to the development of the Convention[8] through the PC-CY Committee. Since then several versions have been developed until a final version was published in June 2001[9] following the approval of the European Committee on Crime Problems (CDPC).[10] The Council of Europe Ministers' Deputies approved the Convention in September 2001.[11] This was followed by a formal adoption by the Foreign Affairs Ministers meeting and opening up the Convention to signatures in November 2001.

Following the first five ratifications, the Cyber-Crime Convention came into force on 01 July, 2004. As of May 2008, the signing and ratification process for the CyberCrime Convention resulted with 39 member states (plus the external supporters United States, Canada, South Africa, Japan, and Montenegro) signing and 22 countries (Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine, and United States of America[12]) ratifying the main convention out of the potential 50 countries (45 CoE member states plus the above mentioned external supporters).

---

6 The text of the Convention can be found at http://conventions.coe.int/treaty/en/projects/cybercrime.htm.

7 European Commission, Interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet, Version 7 (June 4, 1997).

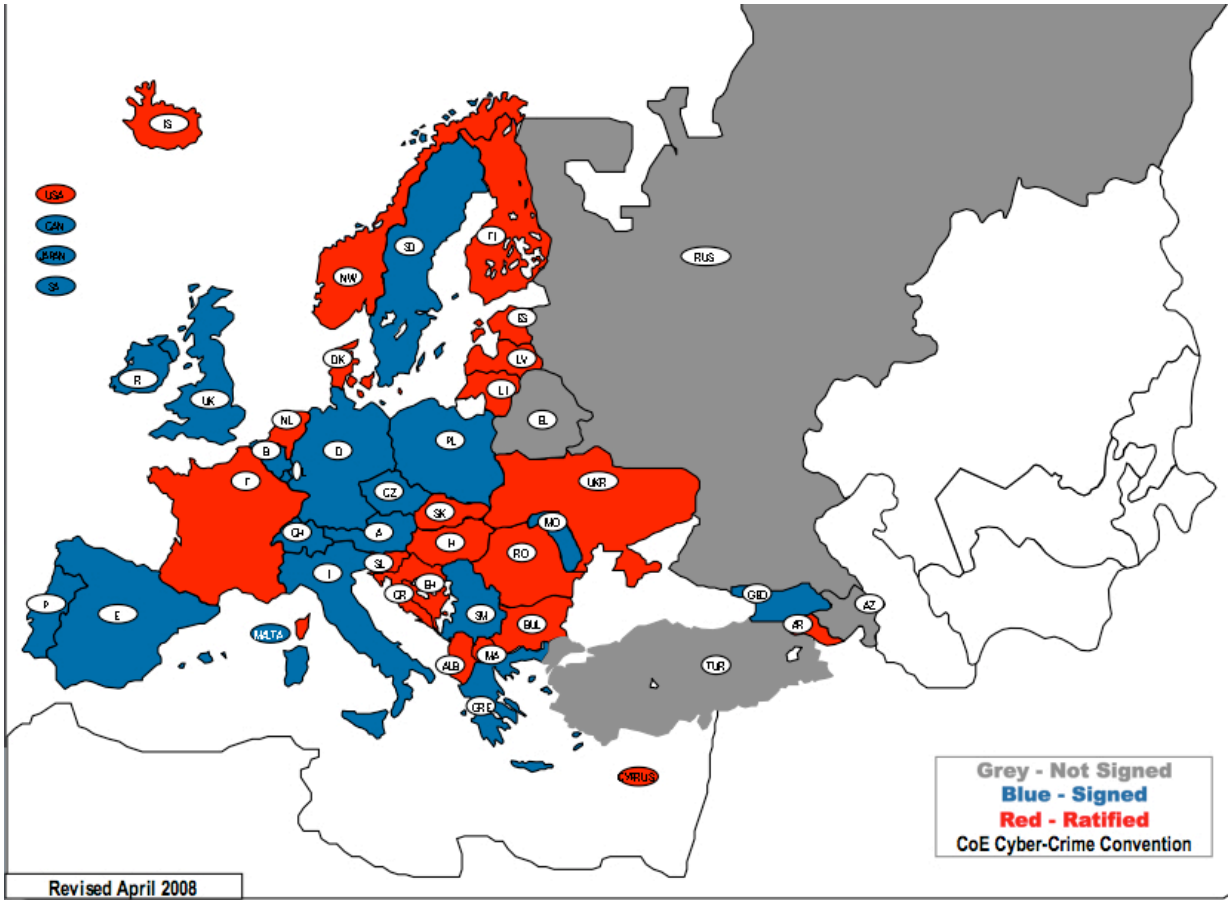
8 The United States was invited to participate as an "observer" in both the 1989 and 1995 Recommendations, as well as in the development of the Convention on Cyber Crime. See Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice, Frequently Asked Questions and Answers1 About the Council of Europe Convention on Cybercrime, (Final Draft, released June 29, 2001), at http://www.cybercrime.gov/newCOEFAQs.html.

9 European Committee on Crime Problems (2001) 'Committee of Experts on Crime in Cyberspace (PC-CY)', Final Draft Convention on Cyber-crime,' CDPC (2001) 17, Strasbourg, 29 June 2001, at http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm See also the European Committee on Crime Problems, Explanatory Memorandum related to the Cyber-Crime Convention, CDPC (2001) 17, Strasbourg, 29 June 2001, at http://www.privacyinternational.org/issues/cybercrime/coe/cybercrimememo-final.html.

10 An intergovernmental expert body reporting to the Council of Europe's Committee of Ministers.

11 CoE press release, First international treaty to combat crime in cyberspace approved by Ministers' Deputies - 646a(2001), Strasbourg, 19.09.2001.

12 The US Senate approved the ratification of the CyberCrime Convention on 03 August, 2006. See CNet News, 05 August, 2006, at <http://news.com.com/Senate+ratifies+controversial+cybercrime+treaty/2100-7348_3-6102354.html>



Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems

The committee drafting the Cyber-Crime Convention discussed the possibility of including content-related offences other than child pornography (article 9) within the Convention such as the distribution of racist propaganda through computer systems. However, there was no consensus on the inclusion of such a provision within the Convention:

> "While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds."[13]

Nevertheless, the Parliamentary Assembly of the Council of Europe, in its Opinion 226(2001) concerning the Convention, recommended the immediate development of an additional protocol to the Convention under the title "Broadening the scope of the convention to include new forms of offence", with the purpose of defining and criminalising, inter alia, the dissemination of racist propaganda.

The European Committee on Crime Problems (CDPC) and, its Committee of Experts on the Criminalisation of Acts of a Racist and xenophobic Nature committed through Computer Systems (PC-RX), was handed the task of preparing the additional protocol, dealing in particular with the following issues:

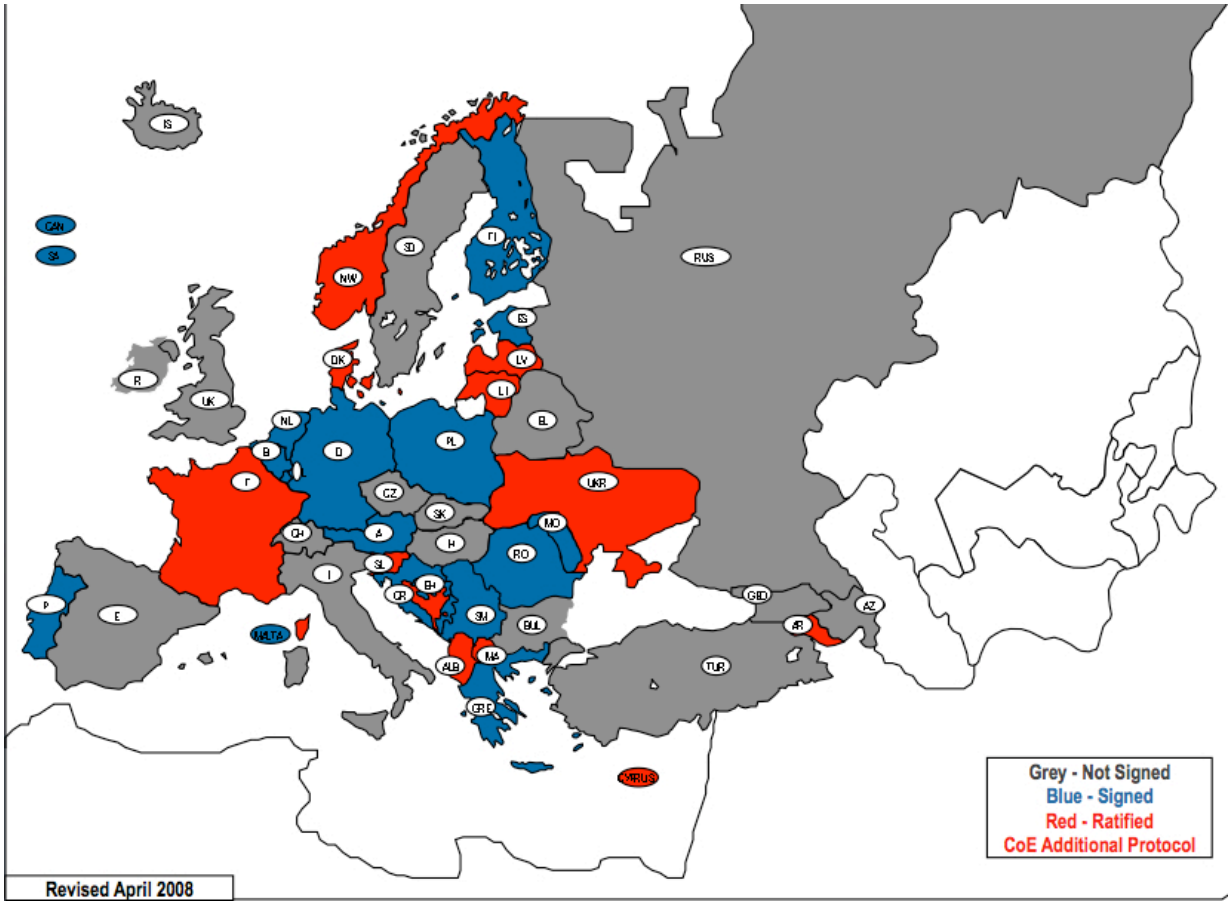
---

13 *Explanatory Report of the* Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, *as adopted by the Committee of Ministers on 7 November 2002, at* http://conventions.coe.int/Treaty/en/Reports/Html/189.htm, para 4.

i. the definition and scope of elements for the criminalisation of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks;
ii. the extent of the application of substantive, procedural and international co-operation provisions in the Convention on Cyber-Crime to the investigation and prosecution of the offences to be defined under the additional Protocol.

The Additional Protocol aims to harmonise substantive criminal law in the fight against racism and xenophobia on the Internet and, to improve international co-operation in this area. The Explanatory Memorandum to the Additional Protocol states that "this kind of harmonisation alleviates the fight against such crimes on the national and on the international level," and that "corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties whose laws in this area are less well defined.

The Additional Protocol was opened for signature in Strasbourg, on 28 January 2003. Since then 32 member states have signed the additional protocol (including the external supporters Canada, Montenegro, and South Africa).[14] Out of the 32 signing states, only 12 member states (Albania, Armenia, Bosnia and Herzegovina, Cyprus, Denmark, France,[15] Latvia, Lithuania, Norway, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia) have ratified the Additional Protocol as of May 2008. The Protocol entered into force following the initial five ratifications on 1 March, 2006.



14 These are Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Poland, Portugal, Romania, Serbia and Montenegro, Slovenia, Sweden, Switzerland, Ukraine. Note that Canada also signed the Additional Protocol.

15 France ratified the Additional Protocol on 10 January, 2006, and will come into force on 01 May, 2006.

Part I – A Critical Assessment of the Cyber-Crime Convention 2001

The Cyber-Crime Convention 2001

The substantive criminal law measures of the Cyber-Crime Convention include offences[16] on intentional illegal access of computer systems,[17] intentional illegal interception of non-public transmissions of computer data,[18] any intentional interference with computer data including deletion or alteration,[19] any intentional interference with a computer system,[20] misuse of certain devices designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5 of the Convention,[21] and the possession of such devices with an intent to committing of such offences.[22] Moreover the Convention includes computer related crimes such as computer related forgery,[23] fraud,[24] and content related offences such as child pornography.[25] Offences related to infringements of copyright and related rights are also included within the Convention.[26]

The procedural law measures of the Convention include conditions and safeguards,[27] expedited preservation of stored computer data,[28] expedited preservation and partial disclosure of traffic data,[29] production orders for law enforcement agencies for accessing data,[30] the search and seizure of stored computer data,[31] real-time collection of traffic data,[32] interception of content data,[33] extradition,[34] principles relating to mutual assistance,[35] and the creation of a 24/7 network of law enforcement point of contacts.[36]

The nature of the CoE policy process – no openness nor transparency

The CoE Committee of Experts on Crime in Cyberspace drawn from 16 member states was working on the Cyber-Crime Convention since September 1997 before the first public release of draft version 19 in April 2000. Although its existence was no secret through references to the draft Convention within

16 Attempt and aiding or abetting of the offences within articles 2-10 are covered within article 11.
17 Article 2, Cyber-Crime Convention.
18 Article 3.
19 Article 4.
20 Article 5.
21 Article 6.
22 Article 6(1)(b).
23 Article 7.
24 Article 8.
25 Article 9.
26 Article 10.
27 Article 15.
28 Article 16.
29 Article 17.
30 Article 18.
31 Article 19.
32 Article 20.
33 Article 21.
34 Article 24.
35 Articles 25-34.
36 Article 35.

publicly available documents at both national[37] and European Union[38] level, the content of the draft Convention was only distributed publicly after April 2000.

Although the draft convention has been published in April 2000, some important parts of the draft convention, namely those related to interception of communications, have not been made publicly available until October 2000, two months before the deadline issued for public comments by the Council of Europe. These important sections were certainly not part of the April 2000 version (No 19) of the draft convention.

Universally accepted process conditions[39] such as openness, and transparency have not been respected at the Council of Europe level during the development of the Convention. An open and transparent policy making would generally lead into easy to understand regulation and legislation with clear aims and objectives. There was limited transparency during the CoE process, and the policy making process would have benefited from greater openness especially in the light of co-operation between member or supporting States and the private industry being encouraged within the Convention.

Hence the CoE process has not been accessible and open and a "dialogue" with all interested parties especially with the representatives of the civil society has not been established at all despite the claims by the Council of Europe that "consultation process proved useful" since the release of the declassified versions of the draft Convention.[40] Submissions made by non governmental organisations were largely ignored by the Council of Europe.

The text of the Convention remains unclear – explanations within the Explanatory Report cannot replace legal clarity

The draft versions of the Convention often referred to the explanatory report that would be published in addition to the Convention. However, the explanatory report was not published in its draft format for public review until 14 February, 2001. The consultation process in relation to the draft versions of the Convention was completed by then. Although the final version of the explanatory memorandum[41] is useful for better understanding of the Cyber-Crime Convention, it should be noted as the Council of Europe document "Introduction to Conventions and Agreements in the European Treaty Series (ETS),"[42] states that:

> "Following the practice instituted by the Committee of Ministers of the Council of Europe in 1965, *explanatory reports* have been published on some of the treaties. These reports, prepared by the committee of experts instructed to elaborate the European Convention or Agreement in question and published with the authorisation of the Committee of Ministers, *might facilitate*

---

37 Draft Council of Europe Convention on Cyber Crime, UK Parliamentary Select Committee on European Scrutiny Twenty-First Report, HC 34-xxi, 21 June 1999. But note that a first reference to the draft Convention and to the work of the PC-CY Committee was made in the European Scrutiny Committee Reports, First Report, 7 December 1998, HC 34-I, Session 1998-99 (High Tech Crime section). Note also the Home Office Press Release: Making The Internet Safe (306/99), 4 October 1999.

38 European Union, Common Position on the COE Convention, 27 May 1999. (Official Journal L 142, 05/06/1999 p. 0001 - 0002) adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe.

39 See for example the European Commission, European Governance paper which refers to similar process conditions at the EU level: COM(2001) 428, Brussels, 25.7.2001. Note also Carter, C.A., "Democratic Governance Beyond the Nation State: Third-Level Assemblies and Scrutiny of European Legislation," (2000) *European Public Law*, (6) 3, 429-459.

40 Paragraph 14 of the Explanatory Report.

41 Explanatory Report of the Council of Europe CyberCrime Convention, at http://conventions.coe.int/treaty/en/Reports/Html/185.htm, 2001.

42 See http://conventions.coe.int/treaty/EN/cadreintro.htm.

> *the application of the provisions of the respective treaties*, although **they do not** constitute instruments providing an authoritative interpretation of them."

As the subject matter of this Convention is pretty complex, the drafters could be criticised for not producing a clear and understandable stand-alone text. The wording of various sections should have been clarified in the main text of the Convention rather than the interpretation being left to instruments and/or reports that will not provide "an authoritative interpretation" of the Convention itself.[43] This view was supported by the Working Party on the protection of individuals with regard to the processing of personal data of the European Commission which concluded that "explanations in the explanatory memorandum cannot replace legal clarity of the text itself."[44] Precision in wording is crucial considering the civil liberties implications of the Cyber-Crime Convention that will be later addressed in this handbook.

Problems associated with the scope of the procedural provisions

Article 14(1) provides that "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." Each Party shall apply the powers and procedures referred to in Article 14(1) to:[45]

> a. the criminal offences established in accordance with articles 2-11 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.

It is however maintained that the scope of the above provisions should have been limited to the offences established in articles 2-11 of this Convention (article 14(1)(a)) and should not have extended to "other criminal offences" (article 14(1)(b)) committed by means of a computer system. It is not at all clear what "other criminal offences" means under article 14(1)(b) and there is no explanation whatsoever why the procedural provisions of the Cyber-Crime Convention should be extended to cover other criminal offences. Although the scope of this section is limited by means of article 21 which "provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law",[46] it still remains unclear why the scope should be extended to criminal offences that are not defined by this Convention.

As a result of the widening of the scope of procedural provisions, search and seizure of computer data measures, interception of communications and traffic data, expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, and production orders (articles 16-21) could be applied to the offences under article 14(1) established not only in accordance with articles 2-11 of this Convention; but also to other criminal offences established by means of a computer system; and to evidence gathering in electronic form of any criminal offence.

It is advised that during the implementation process of the Cyber-Crime Convention, procedural powers and provisions should be limited to the offences included in the Convention only. In any case reservations provided in article 14(3)(a) should be noted:

---

43 Akdeniz, Y., SuperOnline Comments on CoE draft Cyber-Crime Convention version 24REV2, 11 December, 2000 (unpublished)

44 Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime (European Commission) Document adopted by the Data Protection Working Party, March 2001, at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm.

45 Except as specifically otherwise provided in Article 21 (Interception of content data) according to article 14(2).

46 See paragraph 142 of the Explanatory Memorandum. Note also the limitation in relation of article 20 (Real-time collection of traffic data) in article 14(3).

> "each Party may reserve the right to apply the measures referred to in Article 20 (Real-time collection of traffic data) 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 (Interception of content data). Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20 (Real-time collection of traffic data)."

Common Standards and Minimum Safeguards

One major objection to the Convention is that it does not seem to be compatible with the European Convention on Human Rights and with the jurisprudence of the European Court of Human Rights in Strasbourg especially in relation to article 8. The CoE unfortunately failed to explicitly state that the 2001 Convention is compatible with the ECHR and with the jurisprudence of the Strasbourg Court in the preamble of the Cyber-Crime Convention. The preamble of the Convention states that "the member States of the Council of Europe and the other States signatory hereto" are "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…" However, this falls short of addressing concerns especially in relation to article 8 and the related jurisprudence of the European Court of Human Rights.

Powers and procedures provided within the Cyber-Crime Convention are required to be subject to the "conditions and safeguards provided for under the domestic law of each Party" which under article 15(1) should

> "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."[47]

Furthermore, the explanatory memorandum states that "as the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." But although there is reference to common standards or minimum safeguards (such as the ECHR in respect of the members of the CoE), it is not true to say that "there are similar protections provided under the laws of most States."[48] In reality, standards and safeguards vary even within the CoE region despite the existence of the ECHR, and there are several article 8 infringements in relation to interception of communications and surveillance practices used by the members of the CoE.

Rather than leaving the decision making to the parties to the Convention, common safeguards based upon the ECHR and the jurisprudence of the Strasbourg court should have been provided within the 2001 Convention. Stakes are high in terms of infringement of human rights especially in terms of privacy of communications:

> "The legislation of numerous European states fails to comply with Article 8 of the Convention where telephone tapping is concerned. States use--or abuse-- the concepts of official secrets and secrecy in the interests of national security. Where necessary, they distort the meaning and nature of that term."[49]

---

47 See further para 145 of the Explanatory Memorandum.

48 See para 145 of the Explanatory Memorandum.

49 Concurring Opinion of Judge Pettiti in *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91.

Moreover, the issue of data protection has been completely left out to accommodate US interests and not even referred to as a safeguard as will be explained below.

Although the principle of proportionality is mentioned in article 15(1) as another safeguard in terms of powers and procedures to be adopted by the member states, this is inadequate. The explanatory report states that "proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law."[50] While this will be based upon the ECHR principles for the CoE member states, the report states that "other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures."[51] But if individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 8, a legal framework and very strict limits on such powers are called for.[52]

The requirement for the provision of "adequate protection of human rights" in article 15 demands further clarification in relation to the jurisprudence of the European Court of Human Rights in Strasbourg. Therefore, the implementation of article 15 of the Convention by parties to the convention need to be sharper and more explicit in terms of guaranteeing rights to citizens.

Serious lack of commitment to data protection principles

A serious lack of commitment to data protection principles is evident in the Cyber-Crime Convention despite the existence of the 1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[53] and the CoE 1999 Recommendation R(99)5 in relation to privacy on the Internet.[54]

Data protection laws have been in place in many European countries since the publication of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg 1981, European Treaty Series No. 108) by the Council of Europe. All member states of the European Union (and 30 member states of the CoE) currently have data protection laws and the recently established European Union Charter of Fundamental Rights recognises data protection as a fundamental right under article 8:

> "Everyone has the right to the protection of personal data concerning him or her."

The Preamble of the Cyber-Crime Convention states that the member States of the Council of Europe and the other States signatory hereto are "mindful of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," but the provisions of the Convention do not refer to the 1981 Convention. It should also be noted that the earlier draft versions of the Cyber-Crime Convention did not even refer to the 1981 Convention. Only after several calls from civil liberties organisations was the preamble of the Convention revised so as to refer specifically to the standards of protection required by the 1981 CoE Data Protection Convention and this was absent from the publicly available versions 19, 22, and 24REV2.

---

50 Para 146.

51 Para 146.

52 *Camenzind v Switzerland* (Application No. 21353/93), (1999) 28 EHHR 456 and *Funke v. France*, A/256-A, (1993) 16 EHRR 297.

53 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108, Strasbourg, 28 January, 1981.

54 The Council of Europe Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers, Deputies, at http://cm.coe.int/ta/rec/1999/99r5.htm.

It is unsatisfactory that the 1981 Convention and the 1999 Guidelines are not directly referred to within article 15 (Conditions and safeguards) of the Convention as well as within the Preamble of the Cyber-Crime Convention[55] along with the other international instruments to ensure that the Council of Europe, its member states, and future signing states are also committed to data protection and fair privacy practices regarding the Internet as set out by non other than the Council of Europe.

The CoE Recommendation 99(5) sets out important principles of fair privacy practice for users and Internet service providers and is directly related to the purposes of the Cyber-Crime Convention. But it is not even mentioned, it is as if the Convention and the Recommendation have been developed by two completely unrelated separate bodies. On the other hand, such important safeguards are included within other regional and international agreements including the European Union's Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[56] Interference by public authorities should have been also subject to extremely strict conditions and safeguards within the 2001 Convention considering the fact that not all CoE member states have national data protection legislation.[57]

For example, Croatia which signed and ratified the Cyber-Crime Convention, only signed the Data Protection Convention in June 2003 but has not ratified it yet.[58] There is also concern that some member states which did not sign or ratify the Data Protection Convention may sign and ratify the Cyber-Crime Convention and/or the additional protocol prior to introducing data protection laws (for a full list of the status of the ratifications see Appendix I).

On the other hand members of the European Union can only send personal data (in principle) to non-EU states if such states do provide an adequate level of data protection as described in the EU Directive of 95/46/EC. So far the European Commission[59] has ruled that the EU member-states[60] can only send personal data to the following states which provide an adequate protection: Hungary, Switzerland, USA (safe harbour), Canada, and Argentina.

It is regrettable that signing and ratification of the Cyber-Crime Convention is not subject to the provision of legal safeguards on data protection and subject to the ratification of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The exclusion of data protection safeguards was criticised by the Article 29 working party on the protection of individuals with regard to the processing of personal data of the European Commission which stated that "the Council of Europe, in promoting international co-operation in matters of cyber-crime outside its own membership, needs to pay particular attention to the protection of fundamental rights and freedoms, especially the right to privacy and personal data protection." [61] The Article 29 Data Protection Working Party also regretted the fact that "no provision is made on the incrimination of violation of data protection rules"[62] specifically within the Cyber-Crime Convention.

---

55 While the Preamble refers to the 1981 Convention, it does not refer to the 1999 recommendation.

56 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union, 2000/C 197/01. See specifically article 23 of the Convention.

57 30 member states (out of 45) of the Council of Europe have ratified the 1981 Convention. See http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=108&CM=8&DF=.

58 On the other hand, Albania which signed and ratified the Cyber-Crime Convention did not sign nor ratify the 1981 Data Protection Convention but does have a data protection legislation since 1999.

59 See generally the European Commission's adequacy pages at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.

60 As well as the three EEA member countries (Norway, Liechtenstein and Iceland).

61 Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime (European Commission) Document adopted by the Data Protection Working Party, March 2001, at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm.

62 *Ibid*., p 4.

There is also no explanation as to why article 15 does not refer to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[63] and to CoE Recommendation N° R(87) 15 regulating the use of personal data in the police sector (17 September 1987),[64] and Recommendation 1181 (1992) on police co-operation. Moreover, safeguards provided within these instruments are not incorporated into the safeguards and conditions that will be applied to the measures provided in the Cyber-Crime Convention. It is advised that the safeguards provided within these instruments are incorporated to any relevant national legislation during the ratification process.

A Convention developed by the Council of Europe should have given a high priority to data protection issues considering the work done in this field by the Council of Europe[65] and safeguards within the Cyber-Crime Convention should have data protection safeguards incorporated to them explicitly. Such important safeguards within the field of data protection were left out to accommodate the US government's interests which does not favour data protection laws as a policy. Unlike in the European Union (and to most extent within the CoE region), there is no comprehensive data protection legislation in the USA. States within the CoE region should have avoided pandering to what constitutes the lowest common denominator in the field of data protection.

Conditions and Safeguards and Judicial Warrants

Article 15(2) of the 2001 Convention states that 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."

One would have expected to see some of the provisions (if not all) such as the production orders (article 18), search and seizure of stored computer data (article 19), real-time collection of traffic data (article 20) and interception of content data (article 21) to be subject to "judicial warrants" as consistent with the jurisprudence of the Strasbourg court. The European Court of Human Rights has clearly laid down in its case law the "requirement of supervision by the judicial authorities in a democratic society, which

---

63 ETS no. 108, Strasbourg, 28 January, 1981.

64 The recommendation has been referred to in two international agreements. Article 115, first paragraph, of the Schengen Agreement states that control by the supervisory authority should take account of the recommendation. The Treaty of Amsterdam incorporated the Schengen Agreement into the EU Treaty. Likewise, in its article 14, paragraph 1, the Europol Treaty provides that processing of police data should take account of the 1987 recommendation of the Council of Europe. The recommendation is at http://www.coe.fr/dataprotection/rec/r(87)15e.htm.

65 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no. 108, Strasbourg, 28 January, 1981; Council of Europe Committee of Ministers Recommendation No R (99) 5 of The Committee of Ministers to Member States for the Protection of Privacy on the Internet: Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways (adopted by the Committee of Ministers on 23 February 1999, at the 660th meeting of the Ministers' Deputies); Council of Europe Committee of Ministers Recommendation No R (95) 4 of The Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (adopted by the Committee of Ministers on 7 February 1995, at the 528th meeting of the Ministers' Deputies); Council of Europe Committee of Ministers Recommendation No R (87) 15 of The Committee of Ministers to Member States regulating the use of personal data in the police sector (adopted by the Committee of Ministers on 17 September 1987, at the 410th meeting of the Ministers' Deputies). Note also *New technologies: a challenge to privacy protection?*, study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989, at http://www.legal.coe.int/dataprotection/Default.asp?fd=pub&fn=NTE.htm; and *Protection of personal data with regard to surveillance*, report by Mr. Giovanni BUTTARELLI, Secretary General of the Italian Data Protection Authority (Italy), 2001, at http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm.

is characterised by the rule of law, with the attendant guarantees of independence and impartiality."[66] It has also been stated that "this is all the more important in order to meet the threat posed by new technologies."[67]

Furthermore as regards to searches and seizure issues in particular,

> "the relevant legislation and practice must afford individuals 'adequate and effective safeguards against abuse'; notwithstanding the margin of appreciation which the Court recognises the Contracting States have in this sphere, it must be particularly vigilant where, the authorities are empowered under national law to order and effect searches without a judicial warrant. If individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 8, a legal framework and very strict limits on such powers are called for."[68]

Therefore, nothing less than judicial supervision as a safeguard for such procedural powers is acceptable during the implementation process by the parties to the convention especially in the absence of a clear definition for what constitutes "independent supervision".

Production Orders and Private Encryption Keys

Under article 18(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

When read together and if implemented into national legislation, articles 18 (production order) and 19 (search and seizure of stored computer data) could be used by law enforcement agencies to request private encryption keys that has been used to secure/encrypt data in a computer system.

But there are serious security concerns associated with the seizure of private encryption keys or government access to keys ("GAK") and such an access could seriously undermine the security of computers and computer data, e-commerce and the integrity of service providers, as well as causing huge potential costs in global key revocation and change. But this serious concern has not been acknowledged or discussed within the Convention nor within the Explanatory memorandum of the Convention.

But clearly the wording of article 18(1)(a) may be used to request "a person 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." Although this may not specifically relate to encryption keys, article 19(4) which requires parties to adopt 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 related" to search and seizure of stored computer data could clearly be used for the purposes of law enforcement access to encryption keys.

Such an access to encryption keys could also infringe important human rights such as privacy of communications and suspect's right not to self-incriminate himself. The requests for private encryption keys with a production order under article 18 could lead into those holding the private encryption keys

---

66 Concurring Opinion of Judge Pettiti in *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91.

67 *Ibid*.

68 *Camenzind v Switzerland* (Application No. 21353/93), (1999) 28 EHHR 456 and *Funke v. France*, A/256-A, (1993) 16 EHRR 297.

self-incriminating themselves. The right to a fair trial under article 6 of the European Convention of Human Rights includes "the right of anyone charged with a criminal offence ... to remain silent and not to contribute to incriminating himself."[69] The forced disclosure of documentation may not be considered as serious as the demand for personal testimony,[70] but it can be personally incriminating as implying the admission of the existence and possession of encryption keys.

Moreover, the European Court of Human Rights reiterates that the right of any "person charged" to remain silent and the right not to incriminate himself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 of the European Convention on Human Rights. Their rationale lies, inter alia, in protecting the "person charged" against improper compulsion by the authorities and thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6.[71]

It should be noted that only a few countries including the UK, India and Malaysia have adopted the powers[72] that are introduced in article 18 and the Council of Europe should have avoided the introduction and encouragement of powers which seems to be incompatible with the European Convention on Human Rights and with the jurisprudence of the European Court of Human Rights as explained above.

Furthermore, as it stands the empowering of competent authorities at the national level to order a "person 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" would be without any clearly defined conditions and safeguards. Of course article 18(2) refers to the powers and procedures referred to in article 18 to be subject to articles 14 and 15. But there is no explicit and specific protection offered to government (law enforcement) access to encryption keys within those provisions.

As it stands the law enforcement agencies would not be required to protect and keep secure any data or private encryption keys obtained from the suspect computers. In those circumstances, the law enforcement agencies should only be in a capacity to request "plain text" but not encryption keys. Paragraph 176 of the Explanatory memorandum, with respect to the modalities of production, states that "parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order." This could include the data or information to be provided in "plain text". But that explanation falls short of addressing the government access to encryption keys issue.

Problems related to interception of communications

Article 20 deals with real-time collection of traffic data and this section requires competent authorities to "compel service providers" to collect or record through application of technical means (article 20(b)(i)) or to co-operate and assist the competent authorities in the collection or recording (article 20(b)(ii)) of "traffic data in real time" associated with specific communications on its territory transmitted by means of a computer system.

---

69 See *Funke v. France* (1993) 16 E.H.R.R. 297.

70 *Saunders v. the United Kingdom*, 17 December 1996, Reports 1996-VI, p. 2064, § 68 and compare *Funke v. France*, 25 February 1993, Series A no. 256-A, p. 22, § 44.

71 *Funke v. France*, 25 February 1993, Series A no. 256-A, p. 22, § 44; *John Murray v. the United Kingdom*, 8 February 1996, Reports of Judgments and Decisions 1996-I, p. 49, § 45; and *Saunders v. the United Kingdom*, 17 December 1996, Reports 1996-VI, p. 2064, § 68; *Serves v. France*, 20 October, 1997, Reports 1997-VI.

72 Electronic Privacy Information Center, Cryptography and Liberty 2000, (http://www.epic.org/reports/crypto2000.html, Washington, 2000).

Article 21 deals with Interception of content data and this provision was kept secret until October 2000 (two months before the deadline provided by the CoE for public comments). Surveillance powers are far the most important provisions of the Convention and the interested parties should have been given more time to consider these provisions at the time.

Article 21(1)(b) requires the empowerment of competent authorities to compel a service provider to (i) collect or record through application of technical means and to (ii) co-operate and assist the competent authorities in the collection or recording of content data in real-time of specified communications transmitted by means of a computer system.

In technical terms, articles 20(1)(b)(ii), and 21(1)(b)(ii) could require Internet Service Providers to install black boxes (US Carnivore like)[73] for directly assisting the law enforcement agencies in the collection or recording of traffic data, and content data. Such a mechanism could result with secret surveillance and interception of all forms of communications including Internet communications and data. Such an interference by a public authority should be subject to extremely strict conditions and safeguards. Also, the scope of such interception need to be clearly defined by law and should be particularly precise.[74] The Strasbourg Court has repeatedly stressed "the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it".[75] This is why the Court must be satisfied that the "secret surveillance of citizens is strictly necessary for safeguarding democratic institutions and that there exist adequate and effective safeguards against its abuse."[76]

Furthermore, there is no mention of how much such capability for real time surveillance could cost the service provider industry.[77] The cost of such interception and monitoring capabilities for service providers is extremely important and the 2001 Convention is partially silent on this issue though its is mentioned that service providers can only be compelled within their existing technical capability under articles 20(1)(b), and 21(1)(b). Reliance on the "existing technical capabilities" may for the moment satisfy industry concerns in relation to the cost issue but in reality and practice this may not satisfy law enforcement agencies. So discussions in relation to the implementation of this requirement into national legislation will undoubtedly be problematic as was witnessed with the enactment of the Regulation of Investigatory Powers Act 2000 in the United Kingdom.

---

73 See FBI's Carnivore Diagnostic Tool at http://www.fbi.gov/hq/lab/carnivore/carnivore.htm; Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. Donald M. Kerr at http://www.fbi.gov/congress/congress00/kerr072400.htm. See further ACLU Comments regarding Carnivore review team draft report, December 2000, at http://www.aclu.org/news/2000/carnivore_comments.html. Department of Justice, Draft Report: Independent Technical Review of the Carnivore System, November 2000, at http://cryptome.org/carnivore-rev.htm. See further EPIC Carnivore FOIA Litigation pages at http://www.epic.org/privacy/carnivore/.

74 *Camenzind v Switzerland*, (Application No. 21353/93), judgment of 16 December 1997, *Kopp v Switzerland*, (Application No. 23224/94), judgment of 25 March 1998 (since telephone tapping constituted a serious interference with private life it had to be based on a law that was particularly precise.); *Valenzuela Contreras v Spain*, (Application No. 27671/95), judgment of 30 July 1998.

75 *Leander v. Sweden* judgment of 26 March 1987, Series A no. 116, § 60; see also the *Klass v. Germany* judgment of 6 September 1978, Series A no. 28, §§ 42 and 49.

76 Concurring opinion of Judge Wildhaber, joined by judges Makarczyk, Türmen, Costa, Tulkens, Casadevall and Weber, *Rotaru v Romania*, (Application no. 28341/95), judgment of 4 May, 2000.

77 In the UK a recent report expects the largest ISPs to provide the capability to intercept all Internet traffic following the enactment of the Regulation of Investigatory Powers Act 2000. The estimate of the cost for a "passive" interception at a single large ISP works out at £1,384,000 for the first year. See The Smith Group Limited Report for the Home Office on technical and cost issues associated with interception of communications at certain Communication Service Providers, CIR221D009-1.1, (19 April 2000), at http://www.homeoffice.gov.uk/oicd/techcost.pdf.

With regard to secret surveillance measures, the European Court of Human Rights has underlined the importance of that concept in the following terms in the *Malone v. the United Kingdom* judgment:[78]

> "The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the 'law', requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention … The phrase thus implies – and this follows from the object and purpose of Article 8 – *that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident …*
> … Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

Furthermore, the decision in the case of *Amann v. Switzerland*[79] should also be recalled. The Court stated that:

> "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."

The jurisprudence of the European Court of Human Rights should be observed while parties to the Cyber-Crime Convention ratify and implement the Convention at the national level as the monitoring of communications can constitute an interference with the right to respect for private life and correspondence in breach of article 8(2) of ECHR, unless it is carried out in accordance with a legal provision capable of protecting against arbitrary interference by the state with the rights guaranteed.[80]

As mentioned by paragraph 215 of the explanatory report, "in the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law." So the exceptions provided for in article 8(2) are to be interpreted narrowly,[81] and the need for them in a given case must be convincingly established. The relevant provisions of domestic law must be both accessible and their consequences foreseeable, in that the conditions and circumstances in which the state was empowered to take secret measures such as telephone monitoring are to be clearly indicated as the European Court of Human Rights held.[82]

In particular, the avoidance of abuse demands certain minimum safeguards, including the conditions regarding the definition of categories of persons liable to have their telephones tapped, and the nature of offences that could give rise to such an order. It should also be noted that "… states do not enjoy unlimited discretion to subject individuals to secret surveillance or a system of secret files. The interest

---

78 *Malone v. the United Kingdom* judgment of 2 August 1984, Series A no. 82, pp. 32-33, §§ 67-68.

79 Application no. 27798/95, European Court of Human Rights judgment, Strasbourg, 16 February 2000

80 Malone v United Kingdom (A/82) (1985) 7 E.H.R.R. 14; *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483.

81 See *Klass and Others v. Germany* (A/28): (1978) 2 E.H.R.R. 214, para. 42.

82 *Kruslin v France* (A/176-B) (1990) 12 E.H.R.R. 547; *Huvig v France*, A/176-B, (1990) 12 EHHR 528; *Halford v. United Kingdom*, (Application No. 20605/92), Judgment of June 25, 1997, 24 E.H.R.R. 523; *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483.

of a State in protecting its national security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life."[83]

The signing states need to carefully consider and take into account the work and jurisprudence of the European Court of Human Rights in relation to article 8 [84] while developing the conditions and safeguards in relation to the implementation of the Cyber-Crime Convention.

Obligation of confidentiality

Articles 20(3) and 21(3) require signing states to adopt such legislative and other measures as may be necessary to "oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in" articles 20 (real-time collection of traffic data) and 21 (interception of content data).[85]

In the *Valenzuela Contreras v Spain* judgment,[86] the Strasbourg Court recognised that "where a power of the executive is exercised in secret the risks of arbitrariness are evident. In the context of secret measures of surveillance or interception by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures.[87] It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated."[88]

Moreover, such requirements for confidentiality may only be justified for matters to do with national security. So far as the activities of intelligence services are concerned, the Strasbourg court reiterates that "powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[89] However, even concerns for national security do not provide a blanket right for secret surveillance of citizens by the state and "in respect of national security as in respect of other purposes, there has to be at least a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate.

In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities.

---

83 Concurring opinion of Judge Wildhaber, joined by judges Makarczyk, Türmen, Costa, Tulkens, Casadevall and Weber, *Rotaru v Romania*, (Application no. 28341/95), judgment of 4 May, 2000.

84 Note further the Council of Europe Recommendation on the Protection of Privacy on the Internet No R (99) 5 of the Committee of Ministers to Member States which has not been referred at all in the 2001 Convention, at http://www.coe.fr/cm/ta/rec/1999/99r5.htm.

85 Within this context the February 1999 Recommendation of the Council of Europe "for the Protection of Privacy on the Internet" should also be taken into account while developing a policy for the ISPs. See Council of Europe Recommendation (No R (99) 5 of the Committee of Ministers to Member States, at http://www.coe.fr/cm/ta/rec/1999/99r5.htm. Part III paragraph 2 of the recommendation states that ISPs should "Inform users of privacy risks presented by use of the Internet before they subscribe or start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of data."

86 Application No. 27671/95, (1999) 28 EHRR 483.

87 See *Malone v United Kingdom* (A/82) (1985) 7 E.H.R.R. 14, *Kruslin v France*, A/176-A, (1990) 12 EHRR 547, *Halford v. United Kingdom*, (Application No. 20605/92), Judgment of June 25, 1997, 24 E.H.R.R. 523, *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91.

88 *Huvig v France*, A/176-B, (1990) 12 EHHR 528; *Kruslin v France*, A/176-A, (1990) 12 EHRR 547; *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91.

89 See the *Klass and Others v. Germany*, p. 21, § 42; *Rotaru v Romania*, (Application no. 28341/95), judgment of 4 May, 2000.

Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, *inter alia*, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.[90]

Preservation Orders

The Cyber-Crime Convention does not include data retention provisions and instead opted for measures involving data preservation within article 16 (Expedited preservation of stored computer data), and article 17 (Expedited preservation and partial disclosure of traffic data) having not reached a consensus on the retention of traffic data issue.[91]

Under a data preservation regime, upon the request of appropriate authorities, data relating to named suspects could be ordered to be preserved for possible later access following a further disclosure order. Such a case by case basis approach is better than a blanket data retention regime. However, it should be noted that post September 11, policy initiatives within the European Union encourage "data retention" policies rather than "data preservation" as a tool for law enforcement.[92]

Though data preservation itself represents an 'entirely new legal power or procedure in domestic law'[93] for most European countries, nevertheless, data preservation measures 'do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities.'[94] They are also limited 'for the purpose of specific criminal investigations or proceedings'.[95] Such data would be preserved for a period of time as long as necessary, up to a maximum of 90 days.[96]

The Convention furthermore enables through article 20 real-time collection of traffic data 'associated with specified communications' as mentioned above. But these powers do not intrude as far as general data retention policies would:[97]

---

90 *Klass v. Germany* judgment of 6 September 1978, Series A no. 28, pp. 25-26, § 55

91 Note para 135 of the explanatory memorandum. See the Opinion 5/2002 of the Article 29 Data Protection Working Party on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, WP 61, 2 July, 2002, at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp61_en.pdf. Note also the International Working Group on Data Protection in Telecommunications Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe adopted at the 28th meeting of the Working Group on 13./14. September 2000 in Berlin at http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm. Note also Walker, C., & Akdeniz, Y., "Anti-Terrorism laws and data retention: war is over?" (2003) *Northern Ireland Legal Quarterly*, 54(2), Summer, 159-182, at http://www.cyber-rights.org/documents/data_retention_article.pdf.

92 See article 15 of the Directive 2002/ /EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, June 2002.

93 See paragraph 155 of the Explanatory Report of the Council of Europe CyberCrime Convention, http://conventions.coe.int/treaty/en/Reports/Html/185.htm, 2001. Data preservation as opposed to data retention is also supported as a preferred option by the UK All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, http://www.apig.org.uk/APIGreport.pdf, para. 189.

94 *Ibid*, at para 152.

95 See article 14(2) of the Council of Europe CyberCrime Convention, ETS No 185, 2001.

96 *Ibid.*, article 16(2).

97 See para. 219 of the Explanatory Report of the Council of Europe CyberCrime Convention, 2001.

> '… the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.'

Furthermore, while the Explanatory Report of the Cyber-Crime Convention claims the privacy interests arising from the collection of traffic data are diminished compared to the interception of content data, it nevertheless acknowledges that

> '...a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context.'[98]

Mutual Assistance and Dual-Criminality

Article 25(1) requires parties to the Convention to "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." This will 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" under subsection (4).

The crucial issue in relation to mutual assistance is "dual criminality" as a safeguard - that the legal systems of the parties to a mutual assistance request (both the country requesting information and the requested party) have equivalent offences within their national legal systems in relation to the alleged offences that are part of the investigation. It is not acceptable for a law enforcement body of one nation to respond to a request of another without the need for dual criminality safeguards. In the absence of dual criminality, the implementation of this section could lead into the investigation of one nation's law abiding citizens by another nation's law enforcement bodies.

Article 25 is vague and such wording as "the parties shall afford one another mutual assistance to the widest extent possible" could have been clearer and the extent of such assistance should have been defined within this section and should be consequently defined by law. Furthermore, such provisions need to be in accordance with the CoE Convention on Mutual Assistance in Criminal Matters, as well as with the First Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters,[99]and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters,[100] which broadens the range of situations in which mutual assistance may be requested and making the provision of assistance easier, quicker and more flexible. The second additional protocol also takes account of the need to protect individual rights in the processing of personal data.

On the other hand, article 29 dealing with the expedited preservation of stored computer data states in subsection (1) that

> "a Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual

---

98 *Ibid*, at para 227.

99 ETS No. 99, came into force in 1982.

100 ETS No. 182. Opened to signature in November 2001. Only 21 member states signed it and 2 ratified it (Albania and Denmark) – not in force yet.

assistance for the search or similar access, seizure or similar securing, or disclosure of the data."

But subsection 3 of the same section explicitly states that for the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. The only safeguard provided for such requests is under subsection (4) which states that parties can only reserve the right to refuse the request for preservation in respect of offences other than those established in accordance with Articles 2 – 11 of this Convention under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. Mutual assistance can also be refused in relation to political offences or offences which are connected with a political offence as well as in cases in which the execution of the request is likely to prejudice the sovereignty, security, ordre public or other essential interests of the requested state.[101]

Mutual assistance regarding surveillance measures

Provisions to do with mutual assistance regarding the real-time collection of traffic data, and regarding the interception of content data are respectively provided in articles 33 and 34. Article 33 requires parties to the Convention to "provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications". Article 33(2) states that "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, on the other hand, requires parties to the Convention to "provide mutual assistance to each other in the real-time collection or recording of content data of specified communications" to the extent permitted under their applicable treaties and domestic laws.

But neither the general principles relating to mutual assistance provided in articles 23 and 25, nor the procedures pertaining to mutual assistance requests in the absence of applicable international agreements provided in article 27 refer to data protection safeguards in relation to the use and exchange of data in the law enforcement sector. Safeguards in relation to mutual assistance regarding surveillance measures should have been incorporated to these sections as in the EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[102] The EU Convention was the first convention on judicial co-operation in criminal matters that has incorporated rules on protecting information provided by the intercepting Member State when personal data exchanged between two or more Member States. The Council of the European Union saw a need for these rules, particularly given the inclusion in the Convention of certain methods of investigation which are not exclusively judicial.[103]

Data protection provisions are also incorporated to the Schengen Agreement, and the related Convention of June 1990.[104] Moreover, significant work of the CoE conducted in this field including

---

101 See article 29(5).

102 Established by the Council in accordance with Article 34 of the Treaty on European Union. Official Journal C 197 , 12/07/2000 P. 0003 – 0023.

103 See further the Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (Text approved by the Council on 30 November 2000), Official Journal C 379 , 29/12/2000 P. 0007 – 0029.

104 See article 26 of the Convention.

the CoE Recommendation N° R(87) 15[105] regulating the use of personal data in the police sector has been referred to in the Schengen Agreement,[106] and in the Europol Treaty.[107]

CoE Recommendation 1181(1992) on police co-operation and protection of personal data in the police sector, and second evaluation report of the Recommendation[108] should also be noticed. The principles within these documents (developed by no other than the Council of Europe) should have been incorporated to the Title 3 (General principles relating to mutual assistance), Title 4 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements), and to the specific provisions under section 2 (articles 29-34) of the 2001 Convention.

The following points made in the Project Group on Data Protection (CJ-PD) report[109] need to be taken into account while member states ratify the Cyber-Crime Convention:

> the identification of targets of criminal intelligence, either in a substantive way, defining criteria in the law, or in a procedural way, defining the authorities and the circumstances that can give rise to the collection of criminal intelligence;
> the time limit for storing criminal intelligence data after which the data should be reviewed or deleted;
> the use of data about unsuspected persons, collected in the course of the investigation of a specific offence, for the investigation of other unrelated offences;
> the matching of data from open sources, such as the Internet or public files, with police data in order to find data about persons who were not suspected beforehand;
> the notification of the persons about whom data are stored by the police;
> the storage and use of genetic data with a view to the identification of criminals;
> the establishment of a supervisory authority for the protection of personal data held by the police;
> instruments for monitoring development in the use of investigative methods involving the collection, storage and use of personal data.

It is recognised that adequate police powers are necessary to allow the police to fulfil their tasks. However, as the CJ-PD report states, "these powers, to be adequate, necessarily interfere with the respect for private life and should therefore be restricted to the extent that is necessary." In this respect the implementation of the following principles is of the utmost importance so far as the ratification of the Convention by the member states is concerned:[110]

> data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date ;
> they should be screened before they are stored ;
> an individual should have the right to know whether personal data concerning him are kept ;
> he should have an appropriate right of access to such data ;

---

105 17 September 1987. See the recommendation at http://www.coe.fr/dataprotection/rec/r(87)15e.htm. The principles contained in this Recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing.

106 Article 115, first paragraph, of the Schengen Agreement states that control by the supervisory authority should take account of the recommendation. The Treaty of Amsterdam incorporated the Schengen Agreement into the EU Treaty.

107 In its article 14, paragraph 1, the Europol Treaty provides that processing of police data should take account of the 1987 recommendation of the Council of Europe.

108 Adopted on 28 October 1999.

109 The full report is available at http://www.coe.fr/dataprotection/Etudes_Rapports/evaluation_E98_R(87)15.htm.

110 Council of Europe Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector.

> he should have the right to challenge such data and, if necessary, have them rectified or erased ;
> individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved ;
> there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention.

Not surprisingly, it is difficult to strike the right balance between the interests of the law enforcement agencies and the interests of the individuals and their right to privacy. Although exceptions are allowed for law enforcement purposes within various international conventions, the law enforcement collection, processing, storage, and exchange of data should still be subject to rules and such standards already exist. It is a pity that the above mentioned standards were largely ignored, and not explicitly incorporated to the Cyber-Crime Convention.

Provision of Spontaneous information

Article 26(1) states that "A Party may, within the limits of its domestic law, 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".

But this provision should not be read as a requirement to conduct policing duty for the benefit of foreign law enforcement agencies. Such a policing activity and disclosure of data (information) by the law enforcement agencies of one State should not be conducted for the benefit of another State in the absence of dual criminality requirements for the offences in question. If no offence is committed in one State, no information should be collected, processed and disclosed to the law enforcement agencies of another State.

Confidentiality requirement within Article 26(2) should be subject to data protection principles and laws as the current requirement for confidentiality only intends to protect the interests of the disclosing state rather than the interests of the persons about whom information has been disclosed to another country.[111] In any case such information should not be disclosed spontaneously to any state which has no comprehensive data protection legislation in place if and when they sign and ratify the Cyber-Crime Convention. Countries that data should not be disclosed are currently:

> Andorra, Armenia, Croatia, Georgia, Moldova, Turkey, Ukraine, South Africa, and United States of America[112]

Part II – A Critical Assessment of the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

The Additional Protocol was opened for signature in Strasbourg, on 28 January 2003. Since then 32 member states have signed the additional protocol (including the external supporters Canada, and South Africa).[113] Out of the 32 signing states, 12 Member States (Albania, Armenia, Bosnia and Herzegovina,

---

111 Note paragraph 261 of the Explanatory memorandum on this issue.

112 US Department of State press release, Bush Asks Senate Approval to Ratify Convention on Cybercrime, 17 November, 2003, at http://usinfo.state.gov/topical/pol/terror/texts/03111704.htm, and http://www.usdoj.gov/criminal/cybercrime/presidentialMemo.htm.

113 These are Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova,

Cyprus, Denmark, France,[114] Latvia, Lithuania, Norway, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia) have ratified the Additional Protocol as of May 2008. The Protocol entered into force following five ratifications on 1 March, 2006.

Fight against racism and xenophobia is not new. There are international instruments such as the Universal Declaration of Human Rights, and the 1966 International Convention of on the Elimination of All Forms of Racial Discrimination which acknowledge and try to address the problem. Council of Europe also published a recommendation on hate speech in October 1997[115] which called upon member states to take appropriate steps to combat hate speech by ensuring that such steps form part of a comprehensive approach to the phenomenon which also targets its social, economic, political, cultural, and other root causes. However, as noted by the explanatory memorandum to the additional protocol, "as technological, commercial and economic developments bring the peoples of the world closer together, racial discrimination, xenophobia and other forms of intolerance continue to exist in our societies."[116] The report also pointed that "the emergence of international communication networks like the Internet provide certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas."[117]

Within this context the important work conducted by the United Nations needs also be noted. In 1963, the United Nations Declaration on the Elimination of All Forms of Racial Discrimination was published. This was followed by the publication of the International Convention on the Elimination of All Forms of Racial Discrimination in 1965. In 1981 a Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief was also published.

More recently, in August 2001 the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance took place. The final report[118] of the conference expressed deep concern about the use of new information technologies, such as the Internet, "for purposes contrary to respect for human values, equality, non-discrimination, respect for others and tolerance, including to propagate racism, racial hatred, xenophobia, racial discrimination and related intolerance, and that, in particular, children and youth having access to this material could be negatively influenced by it."[119] The report among other significant recommendations urged States to

> "implement legal sanctions, in accordance with relevant international human rights law, in respect of incitement to racial hatred through new information and communications technologies, including the Internet, and further urges them to apply all relevant human rights instruments to which they are parties, in particular the International Convention on the Elimination of All Forms of Racial Discrimination, to racism on the Internet"[120]

Netherlands, Poland, Portugal, Romania, Serbia and Montenegro, Slovenia, Sweden, Switzerland, Ukraine. Note that Canada also signed the Additional Protocol.

114 France ratified the Additional Protocol on 10 January, 2006, and will come into force on 1 May, 2006.

115 Recommendation No. R (97)20 on Hate Speech, adopted by the Committee of Ministers of the Council of Europe on 30 October, 1997.

116 *Explanatory Report of the* Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, *as adopted by the Committee of Ministers on 7 November 2002, at* http://conventions.coe.int/Treaty/en/Reports/Html/189.htm, para 2.

117 *Ibid*., para 3.

118 See generally the Report of the World Conference against Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Durban, 31 August - 8 September 2001, A/CONF.189/12, GE.02-10005 (E) 100102, January 2002 at http://www.un.org/WCAR/aconf189_12.pdf.

119 *Ibid*., para 91.

120 *Ibid*., para 145.

The report also called upon the States to consider the following, taking fully into account existing international and regional standards on freedom of expression, while taking all necessary measures to guarantee the right to freedom of opinion and expression:

> a) Encouraging Internet service providers to establish and disseminate specific voluntary codes of conduct and self-regulatory measures against the dissemination of racist messages and those that result in racial discrimination, xenophobia or any form of intolerance
> and discrimination; to that end, Internet providers are encouraged to set up mediating bodies at national and international levels, involving relevant civil society institutions;
> (b) Adopting and applying, to the extent possible, appropriate legislation for prosecuting those responsible for incitement to racial hatred or violence through the new information and communications technologies, including the Internet;
> (e) Considering a prompt and co-ordinated international response to the rapidly evolving phenomenon of the dissemination of hate speech and racist material through the new information and communications technologies, including the Internet; and in this context strengthening international co-operation.[121]

Following from these significant political developments, the Council of Europe decided that in order to investigate and prosecute such persons, international co-operation is vital. But provisions involving the criminalisation of acts of a racist and xenophobic nature committed through computer systems were left out of the Cyber-Crime Convention 2001 as there was no consensus on the inclusion of such provisions.

While European states such as France and Germany strongly supported such inclusion, the United States of America which has been influential in the development of the main Convention opposed the inclusion of speech related provisions apart from child pornography. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention.[122] The Parliamentary Assembly, in its Opinion 226(2001) concerning the Convention recommended the drafting of an additional protocol with the purpose of defining and criminalising, *inter alia*, the dissemination of racist propaganda.[123]

The Parliamentary Assembly considered racism "not as an opinion but as a crime" in its Recommendation 1543 (2001)[124] on Racism and xenophobia in cyberspace. The Parliamentary Assembly also noted that the protocol will "have no effect unless every state hosting racist sites or messages is a party to it."[125]

Purpose of the Additional Protocol

The purpose of this Protocol is twofold. Firstly, it aims to harmonise substantive criminal law in the fight against racism and xenophobia on the Internet. Secondly, it aims to improve international co-operation in this field. The Council of Europe believes that a harmonised approach in domestic laws may prevent misuse of computer systems for a racist purpose.

The Additional Protocol entails an extension of the Convention's scope, including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist and xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour,

---

121 *Ibid*., para 147.

122 *Explanatory Report of the* Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, *as adopted by the Committee of Ministers on 7 November 2002, at* http://conventions.coe.int/Treaty/en/Reports/Html/189.htm, para 4.

123 *Ibid*., para 5.

124 Text adopted by the Standing Committee, acting on behalf of the Assembly, on 8 November 2001.

125 Para 4 of the Recommendation 1543 (2001).

the Protocol aims at improving the ability of the Parties to make use of the procedural provisions of the Cyber-Crime Convention including international co-operation and mutual legal assistance.

Definitions and measures introduced in the Additional Protocol

Article 2 defines "racist and xenophobic material" as

> any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

The definition contained in Article 2 refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, of a racist and xenophobic nature, in such a format that it can be stored, processed and transmitted by means of a computer system.[126]

Measures to be taken at national level are explained in chapter II of the additional protocol.

Article 3 entitled dissemination of racist and xenophobic material through computer systems requires parties to the additional protocol to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the distribution, or otherwise making available, racist and xenophobic material to the public through a computer system. Such conduct needs to be committed intentionally and without right.

Article 3(2) states that parties may reserve the right not to attach criminal liability to such conduct, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. Moreover, article 3(2) also states that notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 entitled racist and xenophobic motivated threat requires parties to the additional protocol to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the following conduct:

> threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

As in article 3 such conduct needs to be committed intentionally and without right. But unlike in article 3, no exceptions are provided for this offence and parties may not reserve the right not to attach criminal liability to such conduct.

Racist and xenophobic motivated insults are dealt win article 5 which requires the criminalisation of the following conduct by the parties to the additional protocol:

> insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if

[126] Para 12 of the expl. Rep.

used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

As in articles 3 and 4 such conduct needs to be committed intentionally and without right. Parties to the protocol however may under subsection 2 either

(a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or
(b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Finally, article 7 requires parties to the protocol 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, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Article 8 of the Additional Protocol requires Parties to extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Cyber-Crime Convention, to Articles 2 to 7 of this Protocol.

Problems Associated with the Additional Protocol

Harmonisation and Concerns for Freedom of Expression

A Committee on Legal Affairs and Human Rights Report reminded that "racist discourse on the Internet is on the increase and needs to be specifically addressed by the criminal law. The Internet permits a degree of trivialisation of racist and xenophobic discourse, particularly among the young, that would virtually never be achieved through more conventional media. At the same time, the Internet enables veritable racist and xenophobic communities to be formed which cannot be tolerated in its midst by a democratic society."[127] Therefore, with the advancement of new technologies and the Internet, the cultural, moral, and legal differences are more evident than ever.

Differing views of the limits to freedom of expression have produced different legal responses to racist and xenophobic discourse in North America (especially the United States) and in Europe. The recent prosecution of Yahoo in France (Tribunal de Grande Instance de Paris)[128] and the subsequent court case in San Jose (United States District Court for the Northern District of California)[129] is a good example of the differences in legal approaches and protection provided to expression. While such differences are legitimate and acceptable, enforcement of such local and national standards to a person or ISP or company based in another jurisdiction remains problematic but at the same time "states within Western Europe should especially avoid pandering to the lowest common denominator where the least tolerant [such as France and Germany] can set the pace."[130]

---

127 Ibid. para 7.

128 *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000.

129 *YAHOO! Inc. v. La Ligue Contre Le Racisme Et, L'antisemitisme*, Case Number 00-21275 JF, United States District Court For The Northern District Of California, San Jose Division, 145 F. Supp. 2d 1168; 2001 U.S. Dist. LEXIS 7565; 29 Media L. Rep. 2008, June 7, 2001, Decided; *YAHOO!, Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme*, Case Number C-00-21275 JF [Docket No. 17], United States District Court for the Northern District of California, SAN JOSE DIVISION, 169 F. Supp. 2d 1181; 2001 U.S. Dist. LEXIS 18378, November 7, 2001, Decided, at < http://www.cdt.org/jurisdiction/011107judgement.pdf>.

130 Brackets added by the author. Walker, C., & Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp 5-19, at page 14.

The Internet is not a lawless place but if the international norms are developed by adhering to the rules and laws of the lowest common denominator, then such actions (including cases like Yahoo) will have a chilling effect on cyber-speech.

Internet Service Providers Liability

"All the offences contained in the Protocol must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Protocol, as those of the Convention, agreed that the exact meaning of 'intentionally' should be left to national interpretation." [131]

Persons cannot be held criminally liable for any of the offences in this Protocol, if they do not possess the required intent and this includes the Internet Service Providers.

It is not sufficient, for example, for a service provider to be held criminally liable under the provisions of the Additional Protocol, that such a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.[132] Although European Union member states are prevented from imposing a monitoring obligation on service providers with respect to obligations of a general nature under the EU Directive on electronic commerce,[133] this "does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation."[134]

Within this context, principle 6 of the CoE Declaration entitled Freedom of communication on the Internet adopted by the Committee of Ministers on 28 May 2003[135] should be noted:

> Principle 6: Limited liability of service providers for Internet content
> Member States should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.
> Member States should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.
> In cases where the functions of service providers are wider and they store content emanating from other parties, member States may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.
> When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the

---

131 See generally para 25 of the explanatory report.

132 See further Parliamentary Assembly, Committee on Legal Affairs and Human Rights Report on the Draft additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Doc. 9538 5 September 2002 (Rapporteur: Mr Ignasi Guardans, Spain, Liberal, Democratic and Reformers' Group).

133 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") OJ L 178 17 July 2000 p.1

134 See paragraph 47 and 48 of the preamble of the Directive on electronic commerce and article 15 of that Directive.

135 At the 840th meeting of the Ministers' Deputies and explanatory note, H/Inf (2003)7.

information available in the first place, as well as the corresponding right of users to the information.
In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

These are also consistent with the requirements of the European Union Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").[136]

Margin of Appreciation

Article 10 of the ECHR recognises the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas. "Article 10 of the ECHR is applicable not only to information and ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. However, the European Court of Human Rights held that the State's actions to restrict the right to freedom of expression are properly justified under the restrictions of paragraph 2 of Article 10 of the ECHR, in particular when such ideas or expressions violated the rights of others.

The Explanatory Report of the Additional Protocol states that "this Protocol, on the basis of national and international instruments, establishes the extent to which the dissemination of racist and xenophobic expressions and ideas violates the rights of others." But it should also be noted that the European Court of Human Rights has consistently held that:
"the Contracting States enjoy a certain margin of appreciation in assessing the need for an interference, but this margin goes hand in hand with European supervision, whose extent will vary according to the case."[137]

Where there has been an interference with the exercise of the rights and freedoms guaranteed in Article 10(1), the supervision must be strict, because of the importance of the rights in question. Therefore, the necessity for restricting them must be convincingly established.[138] At the same time there is little scope for restrictions under Article 10(2) on political speech or on debate of matters of public interest.[139] But criminalisation of speech which incite violence against an individual or a public official or a sector of the population is deemed to be compatible with article 10.[140] In such cases the State authorities enjoy a wider margin of appreciation when examining the need for an interference with freedom of expression, and it does remain open for competent state authorities to adopt measures, even of a criminal law nature, intended to react appropriately to such remarks.

---

136 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities, vol 43, OJ L 178 17 July 2000 p.1. Note also Common Position (EC) No 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive on electronic commerce, Official Journal C 128 , 08/05/2000 p. 0032 – 0050.

137 *Autronic AG* judgment of 22 May 1990, Series A No. 178, § 61.

138 *Ibid*.

139 *Erdogdu and Ince v. Turkey*, 8 July 1999, Application Nos. 25067/94 and 25068/94 (European Court of Human Rights); *Surek and Ozdemir v. Turkey*, 8 July 1999, Application Nos. 23927/94 & 24277/94 (European Court of Human Rights).

140 See cases such as *Sener v. Turkey*, 18 July 2000, Application No. 26680/95 (European Court of Human Rights).

The European Court of Human Rights in its *Jersild v. Denmark*[141] decision noted the particular importance of combating racial discrimination. In this case it was particularly significant that the applicant did not make the statements himself but assisted in their dissemination in his capacity as a journalist for a news programme.

> "... freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress. Subject to paragraph 2 of Article 10 [of the European Convention on Human Rights], it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance or broadmindedness without which there is no democratic society." [142]

Within this context, the press plays an important role in a democracy as a public watchdog; its duty is to impart information and ideas on all matters of public interest and the public has a right to receive it. These principles apply equally to the audio-visual media. In considering the duties and responsibilities of a journalist, the potential impact of the medium concerned is an important factor; the audio-visual media have a more immediate and powerful effect than the print media does.

The state action should clearly distinguish the categories of speech that could be affected by the provisions of the additional protocol. Political speech regardless of its disturbing, shocking, or offending nature should remain protected.

Denial, gross minimisation, approval or justification of genocide or crimes against humanity

The Additional Protocol includes offences related to the denial, gross minimisation, approval or justification of genocide or crimes against humanity within article 6 which requires the criminalisation of the following conduct by the parties to the additional protocol:

> distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

Within the Council of Europe, only France, Germany, Belgium, Switzerland, and Austria have laws criminalising the denial of crimes against humanity, and in the case of Germany, Belgium, and Austria this is only limited to the denial of genocide committed by the Nazis.[143] The European Court of Human Rights in *Lehideux and Isorni*[144] has made it clear that the denial or revision of "clearly established historical facts – such as the Holocaust (whose negation or revision) would be removed from the protection of Article 10 by Article 17" of the ECHR. The Court stated that "there is no doubt that, like any other remark directed against the Convention's underlying values,[145] the justification of a pro-Nazi

---

141 *Jersild v. Denmark*, September 1994, Application No. 15890/89 (European Court of Human Rights)

142 *Castells v. Spain,* App. no.11798/85, Ser.A vol.236, (1992) 14 EHRR 445, § 42. See also *Lingens v Austria*, App. no.9815/82, Ser. A vol.103, (1986) 8 EHRR 407; *Demicoli v Malta,* App. no.13057/87, Ser.A vol.210, (1992) 14 EHRR 47; *Oberschlick v Austria* App. no.11662/85, Ser.A vol.204, (1995) 19 EHRR 389; *Jersild v Denmark,* App. no.15890/88, Ser. A vol.298, (1995) 19 EHRR 1

143 See generally European Commission against Racism and Intolerance (ECRI), Legal Instruments to combat racism on the Internet, report prepared by the Swiss Institute of Comparative Law (Lausanne), CRI (2000)27, Strasbourg, August 2000.

144 judgment of 23 September 1998.

145 See, *mutatis mutandis*, the *Jersild v. Denmark* judgment of 23 September 1994, Series A no. 298, p. 25, § 35.

policy could not be allowed to enjoy the protection afforded by Article 10." Judge Jambrek in his concurring opinion added that:

> "in order that Article 17 may be applied, the aim of the offending actions must be to spread violence or hatred, to resort to illegal or undemocratic methods, to encourage the use of violence, to undermine the nation's democratic and pluralist political system, or to pursue objectives that are racist or likely to destroy the rights and freedoms of others."[146]

But so far, the approach of the EctHR did not result in CoE members implementing laws criminalising this sort of speech, and it remains to be seen whether the additional protocol will achieve this.

A party under article 6(2) may either

> (a) require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
> (b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Effectiveness of the Additional Protocol

The Additional Protocol carries political significance but will the additional protocol have an impact upon reducing the problem of racism and xenophobia on the Internet?

Although state legislation is still a strong option and maybe preferred in most instances, problems associated with the Internet may require the careful consideration of alternatives to state regulation. Due to the global and decentralised nature of the Internet, government regulation may not be the best alternative to tackle global problems, and jurisdictional issues should be taken into account while policies are developed at the state level.

The Yahoo case is an example of the nation-states desire to enforce and apply their national laws to a global and multi-national medium such as the Internet with regards to racism and hate speech. The French approach in that sense is similar to the German approach in which CompuServe[147] was found liable under German criminal law for the distribution of illegal content over the Internet (mainly child pornography).[148] While there is more consensus on the issue of child pornography as illegal content, the same is not true for content that is categorised as hate speech.

The steps taken by Belgium, France, Germany, and Switzerland at the national level have shown their limitations, and an additional protocol aimed at punishing racism on the Internet will have no effect unless every state hosting racist sites or messages is a party to it as rightly stated by a CoE

---

146 See further the *United Communist Party of Turkey and Others v. Turkey* judgment of 30 January 1998, *Reports of Judgments and Decisions* 1998-I, p. 16, § 23.

147 See the Criminal case of Somm, Felix Bruno, File No: 8340 Ds 465 JS 173158/95, Local Court (Amtsgericht) Munich. An English version of the case is available at http://www.cyber-rights.org/isps/somm-dec.htm.

148 "Ex-CompuServe Executive Convicted," *Associated Press* (Berlin), 28 May, 1998. But the decision was eventually quashed in November 1999. "Germany clears Net chief of child porn charges," *The Independent*, 18 November 1999. Another related case is the prosecution of Frederick Toben, a German-born Australian Holocaust revisionist (with an Australian passport) who denied the Holocaust, by the German Bundesgerichtshof (German Federal High Court). This was despite the fact that Toben's website was published and maintained in Australia. See Chidi, G., "Web law blocks growth When in Rome," *InfoWorld*, Vol. 23, Issue 10, March 5, 2001; Gold, S., "German Landmark Nazi Ruling," *Newsbytes*, December 12, 2000.

Recommendation 1543(2001) on Racism and xenophobia in cyberspace.[149] The global, and decentralised nature of the Internet certainly have an impact upon how it is regulated. The alignment of national criminal laws in relation to content (speech) regulation generally seems not to be a feasible option due to the moral, cultural, economic, and political differences between the member states. The different approaches to freedom of expression should also not be forgotten.

It is difficult to speculate how effective will be a regional international effort such as the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Even if all member states of the CoE sign and ratify the additional protocol, the problem may not disappear. This also reflects the true nature of the Internet which includes risks. But how should we deal with such risks? The "one for all" rules advocated by the CoE remains problematic and countries with strong constitutional protection for freedom of expression such as the USA will not be queuing to sign and ratify the additional protocol. In other words there will always be safe havens to host and carry content deemed to be illegal by the additional protocol.

There are other options available to tackle such risks and problems in a global society and the role of individual governments and supranational, and international organisations is still crucial. But this should not be limited to developing international conventions, and adopting laws. Regulation is often designed to reduce risk but alternative methods can be less costly, more flexible and more effective than prescriptive government legislation. These include the option "to do nothing", self-regulation, co-regulation, and information and education campaigns.

Within the context of racism and xenophobia on the Internet, "to do nothing" does not seem to be an appropriate option as the problem does not seem to disappear. In fact the growing concerns for the availability of such content over the Internet triggered the Council of Europe to develop the additional protocol.

The Declaration on Freedom of communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003[150] encourages self-regulation and co-regulatory initiatives regarding Internet content. Similar recommendations were also made in a CoE Recommendation (2001) 8 on self-regulation concerning cyber-content.[151] The no rush to legislation approach adopted by the European Commission with its Action Plan on promoting safer use of the Internet should be applauded which is now extended to cover EU candidate countries. The Action Plan includes research into technical means to tackle both illegal and harmful content, and information and education campaigns.

Therefore, there is more to be done to tackle the problem of racism and xenophobia on the Internet.[152]

---

149 Recommendation 1543 (2001) on Racism and xenophobia in cyberspace, t*ext adopted by the Standing Committee*, acting on behalf of the Assembly, on 8 November 2001.

150 at the 840th meeting of the Ministers' Deputies and explanatory note, H/Inf (2003)7.

151 Recommendation Rec(2001)8 was adopted by the Committee of Ministers on 5 September 2001 at the 762nd meeting of the Ministers' Deputies. See further the Explanatory Memorandum to Recommendation (2001) 8 of the Committee of Ministers to member States on self-regulation concerning cyber content: self-regulation and user protection against illegal or harmful content on new communications and information services.

152 See generally Akdeniz, Y., *Stocktaking on efforts to combat Racism on the Internet*, background report for the High Level Seminar on Racism and the Internet, Intergovernmental Working Group on the Effective Implementation of the Durban Declaration and Programme of Action, Fourth session, Geneva, 16-27 January 2006, E/CN.4/2006/WG.21/BP.1, published by the United Nations High Commissioner for Human Rights (UNHCHR) Office: Geneva, January 2006, 45pp, at <http://www.cyber-rights.org/reports/ya_un_paper_int_06.pdf>.

Conclusion to the Handbook

Although the Cyber-Crime Convention states in the preamble that a proper balance needs to be ensured between the interests of law enforcement agencies and respect for fundamental human rights, the balance is certainly in favour of the law enforcement agencies.

The development of the Internet requires the instillation of trust in Internet users and affirmation that their expectation of privacy in correspondence is legitimate. But it seems to be the Council of Europe which is lacking in trust and instead seeks to encourage surveillance systems into the national legal systems of its member states without due safeguards.

Governments and supranational and international organisations should co-operate to respect fundamental human rights such as freedom of expression and privacy, and should encourage rather than limit the peoples' usage of the Internet through excessive regulation at the national level. Responses to problems that are associated to the Internet need to be proportionate and effective. Otherwise, far from free and unregulated, the Internet may end up as the most regulated medium in history. It should be remembered in the words of Judge Pettiti that "the mission of the Council of Europe and of its organs is to prevent the establishment of systems and methods that would allow 'Big Brother' to become master of the citizen's private life."[153] But the Cyber-Crime Convention unfortunately suggests otherwise.

November 2003 (revised and edited May 2008).

[153] Per Judge Pettiti, concurring opinion in *Malone v United Kingdom* (A/82) (1985) 7 E.H.R.R. 14.

Information About the Author of the Report

Written By: **Dr. Yaman Akdeniz** – is a senior lecturer at the School of Law, University of Leeds where he teaches and writes mainly about Internet related legal and policy issues. Akdeniz is also the founder and director of Cyber-Rights & Cyber-Liberties (UK) <http://www.cyber-rights.org>), a non-profit civil liberties organisation. Dr. Akdeniz is also an international policy fellow of the Open Society Institute working on a project entitled *Civil Society Participation to the policy making process of the Turkish Government in relation to the development of an Information Society in Turkey* between March 2003-March 2004. He has given written and oral evidence on a number of occasions in front of governmental bodies including at the European Union, United Nations, and OSCE level, most recently in front of the European Parliament Temporary Committee on the Echelon interception systems and its threats to human rights. His publications include *Sex on the Net? The Dilemma of Policing Cyberspace* (South Street Press, 1999) *The Internet, Law and Society* (ed. with C. Walker and D. Wall, Longman, 2000); Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] *Criminal Law Review*, (February), pp. 73-90 (with Taylor, N.; Walker, C.); and Walker, C., & Akdeniz, Y., "Anti-Terrorism laws and data retention: war is over?" (2003) *Northern Ireland Legal Quarterly*, 54(2), Summer, 159-182. His forthcoming publications include *Internet Child Pornography and the Law: National and International Responses*, Ashgate, (to be published in 2004). For further information in relation to his work see <http://www.cyber-rights.org/yamancv.htm>.

His contact details are as follows: Dr. Yaman Akdeniz, Faculty of Law, University of Leeds, Leeds LS2 9JT E-mail: lawya@leeds.ac.uk / lawya@cyber-rights.org Tel: + 44 113 3435011

Cyber-Rights & Cyber-Liberties (UK) (http://www.cyber-rights.org) is a non profit organisation established to protect the interests of all honest, law-abiding Internet users with the aim of promoting free speech and privacy on the Internet. It was founded in January 1997 and has been actively involved with the Internet policy-making processes of the UK Government, the European Union, Council of Europe, OECD, and the United Nations. It has also been an active member of the Global Internet Liberty Campaign (http://www.gilc.org) since March 1997, and was involved with the formation of the UK Internet Users Privacy Forum ("IUPF") in March 1999. The organisation also launched the Cyber-Rights.Net project (http://www.cyber-rights.net) in association with HushMail in November 2000.

Resources for activists

Council of Europe Documents and Links

Convention on Cybercrime, ETS No. 185 at http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ETS No: 189 at http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=189&CM=8&DF=

CoE, Human Rights, Media Division pages at http://www.coe.int/T/E/human_rights/media/ and http://www.humanrights.coe.int/media/

Committee of Ministers declaration on freedom of communication on the Internet, adopted on 28 May 2003, H/Inf (2003) 7 eng, http://www.coe.int/T/E/Human_rights/h-inf(2003)7eng.pdf

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108, Strasbourg, 28 January, 1981.

Council of Europe, Communication and Research pages on Cybercrime at http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercrime/Index.asp

Council of Europe Committee of Ministers Recommendation No R (87) 15 of The Committee of Ministers to Member States regulating the use of personal data in the police sector (adopted by the Committee of Ministers on 17 September 1987, at the 410th meeting of the Ministers' Deputies).

Council of Europe Committee of Ministers Recommendation No R (95) 4 of The Committee of Ministers to Member States on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (adopted by the Committee of Ministers on 7 February 1995, at the 528th meeting of the Ministers' Deputies)

Council of Europe Committee of Ministers, Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies), at http://cm.coe.int/ta/rec/1989/89r9.htm

Council of Europe Committee of Ministers, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies), at http://cm.coe.int/ta/rec/1995/95r13.htm

Council of Europe, Legal Affairs Data Protection pages at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

Council of Europe, Legal Affairs, Data Protection provisions around the world at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/National_laws/NATIONAlLAWS-EN.asp

European Commission against Racism and Intolerance (ECRI), Legal Instruments to combat racism on the Internet, report prepared by the Swiss Institute of Comparative Law (Lausanne), CRI (2000)27, Strasbourg, August 2000.

Explanatory Report of the Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, *as adopted by the Committee of Ministers on 7 November 2002, at* http://conventions.coe.int/Treaty/en/Reports/Html/189.htm

Explanatory Report of the Council of Europe CyberCrime Convention, 2001, at http://conventions.coe.int/treaty/en/Reports/Html/185.htm

New technologies: a challenge to privacy protection?, study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989, at http://www.legal.coe.int/dataprotection/Default.asp?fd=pub&fn=NTE.htm

Parliamentary Assembly, Committee on Legal Affairs and Human Rights Report on the Draft additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Doc. 9538 5 September 2002 (Rapporteur: Mr Ignasi Guardans, Spain, Liberal, Democratic and Reformers' Group).

Protection of personal data with regard to surveillance, report by Mr. Giovanni BUTTARELLI, Secretary General of the Italian Data Protection Authority (Italy), 2001, at http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm

Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector.
Recommendation 1543 (2001) on Racism and xenophobia in cyberspace, t*ext adopted by the Standing Committee*, acting on behalf of the Assembly, on 8 November 2001.
Recommendation No. R (97)20 on Hate Speech, adopted by the Committee of Ministers of the Council of Europe on 30 October, 1997.
Recommendation No.R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, *(Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)* at http://www.giodo.gov.pl/Docs/Foreign_Docs/REKOMENDACJE/R(87)15e.htm
Recommendation R(2001)8 was adopted by the Committee of Ministers on 5 September 2001 at the 762nd meeting of the Ministers' Deputies. See further the Explanatory Memorandum to Recommendation (2001) 8 of the Committee of Ministers to member States on self-regulation concerning cyber content: self-regulation and user protection against illegal or harmful content on new communications and information services.
The Council of Europe and the protection of human rights: A 32-page illustrated booklet presenting the vocation and actions of the Council of Europe in the field of human rights: It covers the European Convention on Human Rights, the European Social Charter, the European Convention for the Prevention of Torture, the Framework Convention for the Protection of National Minorities, combating racism and intolerance, equality between women and men, activities in the spheres of media and democracy, human rights awareness, and helping the new democracies in the transitional period. Its format, design and approach combine to make it easy to read and accessible to all. This document is available through http://www.coe.int/T/E/Human_rights/prothre.asp
The Council of Europe Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways, R(99)5 adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers, Deputies, at http://cm.coe.int/ta/rec/1999/99r5.htm
The cybercrime convention : a pioneering effort of wide legal scope: Address by Guy DE VEL, Council of Europe Director General of Legal Affairs at http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercrime/e_DiscoursDeVelNov2001.asp

European Union Documents and Links
European Commission Data Protection pages at http://europa.eu.int/comm/internal_market/privacy/index_en.htm
European Commission decisions on the adequacy of the protection of personal data in third countries at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm
EU Mutual Legal Assistance documents at http://europa.eu.int/comm/justice_home/doc_centre/criminal/assistance/doc_criminal_assistance_en.htm
European Union, Common Position on the CoE Convention, 27 May 1999. (Official Journal L 142, 05/06/1999 p. 0001 - 0002) adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe.
International Working Group on Data Protection in Telecommunications Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe adopted at the 28th meeting of the Working Group on 13./14. September 2000 in Berlin at http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm
Directive 2002/ /EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, June 2002.
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") OJ L 178 17 July 2000 p.1
Common Position (EC) No 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive on electronic commerce, Official Journal C 128 , 08/05/2000 p. 0032 – 0050.

Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (Text approved by the Council on 30 November 2000), Official Journal C 379, 29/12/2000 P. 0007 – 0029.
Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime (European Commission) Document adopted by the Data Protection Working Party, March 2001, at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm
Opinion 5/2002 of the Article 29 Data Protection Working Party on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, WP 61, 2 July, 2002, at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp61_en.pdf

Other Documents and Links

Cyber-Rights & Cyber-Liberties (UK) CyberCrime pages at http://www.cyber-rights.org/cybercrime/
Billet. S.E., Transnational Advocacy and the CyberCrime Convention: A Consideration of lobbying and global governance, prepared for delivery at the 2002 Annual Meeting of the American Political Science Association, September 2002, at http://apsaproceedings.cup.org/Site/papers/040/040002BilletStev.pdf
Civil Liberties, Human Rights Groups Criticise the Draft Convention - Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, 18 October, 2000, at http://www.gilc.org/privacy/coe-letter-1000.html
Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice, Frequently Asked Questions and Answers1 About the Council of Europe Convention on Cybercrime, (Final Draft, released June 29, 2001), at http://www.cybercrime.gov/newCOEFAQs.html
Criminal case of Somm, Felix Bruno, File No: 8340 Ds 465 JS 173158/95, Local Court (Amtsgericht) Munich. An English version of the case is available at http://www.cyber-rights.org/isps/somm-dec.htm
Department of Justice, Draft Report: Independent Technical Review of the Carnivore System, November 2000, at http://cryptome.org/carnivore-rev.htm>
EPIC Carnivore FOIA Litigation pages at http://www.epic.org/privacy/carnivore/
FBI's Carnivore Diagnostic Tool at http://www.fbi.gov/hq/lab/carnivore/carnivore.htm
The Global Internet Liberty Campaign pages at http://www.gilc.org
GILC Members Maintain Opposition to Cyber-Crime Treaty**:** Responding to the latest version of the Council of Europe's Convention on Cyber-Crime, twenty-one GILC member organizations have drafted a new letter dated 12 December, 2000 (http://www.gilc.org/privacy/coe-letter-1200.html) arguing that the treaty's current provisions will continue to violate the rights of Internet users. The letter from the groups also points out the lack of public input in the drafting process.
GILC Members Release Letter Opposing Cyber-Crime Convention. Twenty-eight GILC member organizations from around the world have urged the Council of Europe to reject the current version of its Convention on Cyber-Crime. The letter dated 18 October, 2000 (http://www.gilc.org/privacy/coe-letter-1000.html) from the organizations states that provisions of the treaty runs contrary to internationally accepted human rights norms and would infringe on the free speech and privacy rights of all Internet users.
Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. Donald M. Kerr at http://www.fbi.gov/congress/congress00/kerr072400.htm
League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000.
Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, Durban, 31 August - 8 September 2001, A/CONF.189/12, GE.02-10005 (E) 100102, January 2002 at http://www.un.org/WCAR/aconf189_12.pdf
The Smith Group Limited Report for the Home Office on technical and cost issues associated with interception of communications at certain Communication Service Providers, CIR221D009-1.1, (19 April 2000), at http://www.homeoffice.gov.uk/oicd/techcost.pdf

UK All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, http://www.apig.org.uk/APIGreport.pdf
Walker, C., & Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp 5-19, at page 14.
YAHOO! Inc. v. La Ligue Contre Le Racisme Et, L'antisemitisme, Case Number 00-21275 JF, United States District Court For The Northern District Of California, San Jose Division, 145 F. Supp. 2d 1168; 2001 U.S. Dist. LEXIS 7565; 29 Media L. Rep. 2008, June 7, 2001, Decided.
YAHOO!, Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, Case Number C-00-21275 JF [Docket No. 17], United States District Court for the Northern District of California, SAN JOSE DIVISION, 169 F. Supp. 2d 1181; 2001 U.S. Dist. LEXIS 18378, November 7, 2001, Decided.
US CyberCrime pages at http://www.cybercrime.gov/
Walker, C., & Akdeniz, Y., "Anti-Terrorism laws and data retention: war is over?" (2003) *Northern Ireland Legal Quarterly*, 54(2), Summer, 159-182, at http://www.cyber-rights.org/documents/data_retention_article.pdf
Privacy International pages at http://www.privacyinternational.org. Note especially *Silenced: An International Report on censorship and control of the Internet* at http://www.privacyinternational.org/survey/censorship/index.html, and *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* at http://www.privacyinternational.org/survey/phr2003/
Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime, 07 June, 2001, at http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm

ECHR Cases cited in the Report

Amann v. Switzerland (Application no. 27798/95)
Autronic AG judgment of 22 May 1990, Series A No. 178, § 61.
Camenzind v Switzerland (Application No. 21353/93), (1999) 28 EHHR 456
Castells v. Spain, App. no.11798/85, Ser.A vol.236, (1992) 14 EHRR 445, § 42
Demicoli v Malta, App. no.13057/87, Ser.A vol.210, (1992) 14 EHRR 47
Erdogdu and Ince v. Turkey, 8 July 1999, Application Nos. 25067/94 and 25068/94.
Funke v. France, 25 February 1993, Series A no. 256-A, p. 22, § 44.
Halford v. United Kingdom, (Application No. 20605/92), Judgment of June 25, 1997, 24 E.H.R.R. 523;
Huvig v France, A/176-B, (1990) 12 EHHR 528
Jersild v Denmark, App. no.15890/88, Ser. A vol.298, (1995) 19 EHRR 1
John Murray v. the United Kingdom, 8 February 1996, 1996-I, p. 49, § 45;
Klass v. Germany judgment of 6 September 1978, Series A no. 28, §§ 42 and 49.
Kopp v Switzerland, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91
Kruslin v France (A/176-B) (1990) 12 E.H.R.R. 547
Leander v. Sweden judgment of 26 March 1987, Series A no. 116, § 60;
Lingens v Austria, App. no.9815/82, Ser. A vol.103, (1986) 8 EHRR 407
Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, pp. 32-33, §§ 67-68.
Oberschlick v Austria App. no.11662/85, Ser.A vol.204, (1995) 19 EHRR 389
Rotaru v Romania, (Application no. 28341/95), judgment of 4 May, 2000.
Saunders v. the United Kingdom, 17 December 1996, Reports 1996-VI, p. 2064, § 68
Sener v. Turkey, 18 July 2000, Application No. 26680/95.
Serves v. France, 20 October, 1997, Reports 1997-VI.
Surek and Ozdemir v. Turkey, 8 July 1999, Application Nos. 23927/94 & 24277/94.
United Communist Party of Turkey and Others v. Turkey judgment of 30 Jan. 1998, 1998-I, p. 16, § 23.
Valenzuela Contreras v Spain, (Application No. 27671/95), judgment of 30 July 1998.

Appendices

Appendix I – Table of signatures and ratification of CoE Conventions

This table is up-to-date as of 05/05/2008.

States	Data Protection Convention	Cyber-Crime Convention	Additional Protocol
Albania	Signed and ratified	Signed and ratified	Signed and ratified
Andorra	Signed but not ratified	Not signed nor ratified	Not signed nor ratified
Armenia	Not signed nor ratified	Signed and ratified	Signed and ratified
Austria	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Azerbaijan	Not signed nor ratified but does have a data protection legislation	Not signed nor ratified	Not signed nor ratified
Belgium	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Bosnia and Herzegovina	Signed and ratified	Signed and ratified	Signed and ratified
Bulgaria	Signed and ratified	Signed and ratified	Not signed nor ratified
Croatia	Signed and ratified	Signed and ratified	Signed but not ratified yet
Cyprus	Signed and ratified	Signed and ratified	Signed and ratified
Czech Republic	Signed and ratified	Signed but not ratified yet	Not signed nor ratified
Denmark	Signed and ratified	Signed and ratified	Signed and ratified
Estonia	Signed and ratified	Signed and ratified	Signed but not ratified yet
Finland	Signed and ratified	Signed and ratified	Signed but not ratified yet
France	Signed and ratified	Signed and ratified	Signed and ratified
Georgia	Signed and ratified	Not signed nor ratified	Not signed nor ratified
Germany	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Greece	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Hungary	Signed and ratified	Signed and ratified	Not signed nor ratified
Iceland	Signed and ratified	Signed and ratified	Signed but not ratified
Ireland	Signed and ratified	Signed but not ratified yet	Not signed nor ratified
Italy	Signed and ratified	Signed but not ratified yet	Not signed nor ratified
Latvia	Signed and ratified	Signed and ratified	Signed and ratified
Liechtenstein	Signed and ratified	Signed but not ratified yet	Not signed nor ratified
Lithuania	Signed and ratified	Signed and ratified	Signed and ratified
Luxembourg	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Malta	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Moldova	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Monaco			
Montenegro	Signed and ratified	Signed but not ratified	
Netherlands	Signed and ratified	Signed and ratified	Signed but not ratified yet
Norway	Signed and ratified	Signed and ratified	Signed and ratified
Poland	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Portugal	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Romania	Signed and ratified	Signed and ratified	Signed but not ratified yet
Russia	Signed but not ratified yet but does have a data protection legislation	Not signed nor ratified	Not signed nor ratified
San Marino	Not signed nor ratified but does have a data protection legislation	Not signed nor ratified	Not signed nor ratified

Serbia and Montenegro	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Slovakia	Signed and ratified	Signed and ratified	Not signed nor ratified
Slovenia	Signed and ratified	Signed and ratified	Signed and ratified
Spain	Signed and ratified	Signed but not ratified yet	Not signed nor ratified
Sweden	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
Switzerland	Signed and ratified	Signed but not ratified yet	Signed but not ratified yet
The former Yugoslav Republic of Macedonia	Signed and ratified	Signed and ratified	Signed and ratified
Turkey	Signed but not ratified	Not signed nor ratified	Not signed nor ratified
Ukraine	Signed but not ratified	Signed and ratified	Signed and ratified
United Kingdom	Signed and ratified	Signed but not ratified yet	Not signed nor ratified

Appendix II Status of the CoE CyberCrime Convention

Convention on Cybercrime
(Convention sur la cybercriminalité)
ETS n° : 185
Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Status as of 05/052008

Opening for signature : Entry into force :
Place : Budapest Conditions : 5 Ratifications including at least 3 member States of the Council of Europe
Date : 23/11/01 **Date : 01/7/2004**

Member States of the Council of Europe:

States	Date of signature	Date of ratification	Date of entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/01	20/06/02	01/7/2004							
Andorra										
Armenia	23/11/01	12/10/2006	1/2/2007							
Austria	23/11/01									
Azerbaijan										
Belgium	23/11/01									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006							
Bulgaria	23/11/01	7/4/2005	1/8/2005		X	X				
Croatia	23/11/01	17/10/02	01/7/2004							
Cyprus	23/11/01	19/1/2005	1/5/2005							
Czech Republic	9/2/2005									
Denmark	22/04/03	21/6/2005	1/10/2005		X			X		
Estonia	23/11/01	12/05/03	01/7/2004				X			
Finland	23/11/01	24/5/2007	1/9/2007							
France	23/11/01	10/01/06	01/05/06							
Georgia										
Germany	23/11/01									
Greece	23/11/01									
Hungary	23/11/01	04/12/03	01/7/2004		X	X	X			
Iceland	30/11/01	29/1/2007	1/5/2007							

Ireland	28/02/02									
Italy	23/11/01									
Latvia	5/5/2004	14/2/2007	1/6/2007							
Liechtenstein										
Lithuania	23/06/03	18/03/04	01/7/2004		X	X	X			
Luxembourg	28/01/03									
Malta	17/01/02									
Moldova	23/11/01									
Monaco										
Montenegro	7/4/2005									
Netherlands	23/11/01	16/11/2006	1/3/2007							
Norway	23/11/01	30/6/2006	1/10/2006							
Poland	23/11/01									
Portugal	23/11/01									
Romania	23/11/01	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005									
Slovakia	4/2/2005	8/1/2008	1/5/2008							
Slovenia	24/07/02	8/9/2004	1/1/2005							
Spain	23/11/01 r									
Sweden	23/11/01									
Switzerland	23/11/01									
the former Yugoslav Republic of Macedonia	23/11/01	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/01	10/3/2006	1/7/2006							
United Kingdom	23/11/01									

Non-member States of the Council of Europe:

States	Date of signature	Date of ratification	Date of entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	23/11/01									
Japan	23/11/01									
South Africa	23/11/01									
United States	23/11/01	29/9/2006	1/1/2007							

Total number of signatures not followed by ratifications :	22
Total number of ratifications/accessions :	22

Notes :
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.
Source: Treaty Office on http://conventions.coe.int

Appendix III Status of the CoE Additional Protocol

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques)
ETS n° : 189
Treaty open for signature by the States which have signed the Treaty ETS 185.

Status as of 05/05/2008

Opening for signature :Entry into force :
Place : StrasbourgConditions : 5 Ratifications.
Date : 28/01/03 Date :

Member States of the Council of Europe:

States	Date of signature	Date of ratification	Date of entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	26/05/03	26/11/2004	1/3/2006							
Andorra										
Armenia	28/01/03	12/10/2006	1/2/2007							
Austria	30/01/03									
Azerbaijan										
Belgium	28/01/03									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006							
Bulgaria										
Croatia	26/03/03									
Cyprus	19/1/2005	23/6/2005	1/3/2006							
Czech Republic										
Denmark	11/02/04	21/6/2005	1/3/2006							
Estonia	28/01/03									
Finland	28/01/03									
France	28/01/03	10/01/06	01/05/06							
Georgia										
Germany	28/01/03									
Greece	28/01/03									
Hungary										
Iceland	09/10/03									
Ireland										
Italy										
Latvia	5/5/2004	14/2/2007	1/6/2007							
Liechtenstein										
Lithuania	7/4/2005	12/10/2006	1/2/2007							
Luxembourg	28/01/03									
Malta	28/01/03									
Moldova	25/04/03									
Monaco										
Montenegro	7/4/2005									
Netherlands	28/01/03									
Norway	29/4/2008	29/4/2008	1/8/2008							

Poland	21/07/03									
Portugal	17/03/03									
Romania	09/10/03									
Russia										
San Marino										
Serbia	7/4/2005									
Slovakia										
Slovenia	26/02/04	8/9/2004	1/3/2006							
Spain										
Sweden	28/01/03									
Switzerland	09/10/03									
the former Yugoslav Republic of Macedonia	14/11/05	14/11/05	1/3/2006							
Turkey										
Ukraine	8/4/2005	21/12/2006	1/4/2007							
United Kingdom										

Non-member States of the Council of Europe:

States	Date of signature	Date of ratification	Date of entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	8/7/2005									
Japan										
South Africa	4/4/2008									
United States										

Total number of signatures not followed by ratifications :	21
Total number of ratifications/accessions :	12

Notes :
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.
Source: Treaty Office on http://conventions.coe.int

Appendix IV - Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Official Journal C 197 , 12/07/2000 P. 0003 – 0023*.

Established by the Council in accordance with Article 34 of the Treaty on European Union

TITLE III - INTERCEPTION OF TELECOMMUNICATIONS

Article 17 - Authorities competent to order interception of telecommunications
For the purpose of the application of the provisions of Articles 18, 19 and 20, 'competent authority' shall mean a judicial authority, or, where judicial authorities have no competence in the area covered by those provisions, an equivalent competent authority, specified pursuant to Article 24(1)(e) and acting for the purpose of a criminal investigation.

Article 18 - Requests for interception of telecommunications
1. For the purpose of a criminal investigation, a competent authority in the requesting Member State may, in accordance with the requirements of its national law, make a request to a competent authority in the requested Member State for:

(a) the interception and immediate transmission to the requesting Member State of telecommunications; or
(b) the interception, recording and subsequent transmission to the requesting Member State of the recording of telecommunications.
2. Requests under paragraph 1 may be made in relation to the use of means of telecommunications by the subject of the interception, if this subject is present in:
(a) the requesting Member State and the requesting Member State needs the technical assistance of the requested Member State to intercept his or her communications;
(b) the requesting Member State and his or her communications can be intercepted in that Member State;
(c) a third Member State which has been informed pursuant to Article 20(2)(a) and the requesting Member State needs the technical assistance of the requested Member State to intercept his or her communications.
3. By way of derogation from Article 14 of the European Mutual Assistance Convention and Article 37 of the Benelux Treaty, requests under this Article shall include the following:
(a) an indication of the authority making the request;
(b) confirmation that a lawful interception order or warrant has been issued in connection with a criminal investigation;
(c) information for the purpose of identifying the subject of this interception;
(d) an indication of the criminal conduct under investigation;
(e) the desired duration of the interception; and
(f) if possible, the provision of sufficient technical data, in particular the relevant network connection number, to ensure that the request can be met.
4. In the case of a request pursuant to paragraph 2(b), a request shall also include a summary of the facts. The requested Member State may require any further information to enable it to decide whether the requested measure would be taken by it in a similar national case.
5. The requested Member State shall undertake to comply with requests under paragraph 1(a):
(a) in the case of a request pursuant to paragraph 2(a) and 2(c), on being provided with the information in paragraph 3. The requested Member State may allow the interception to proceed without further formality;
(b) in the case of a request pursuant to paragraph 2(b), on being provided with the information in paragraphs 3 and
4 and where the requested measure would be taken by it in a similar national case. The requested Member State may make its consent subject to any conditions which would have to be observed in a similar national case.
6. Where immediate transmission is not possible, the requested Member State shall undertake to comply with requests under paragraph 1(b) on being provided with the information in paragraphs 3 and 4 and where the requested measure would be taken by it in a similar national case. The requested Member State may make its consent subject to any condition which would have to be observed in a similar national case.
7. When giving the notification provided for in Article 27(2), any Member State may declare that it is bound by paragraph 6 only when it is unable to provide immediate transmission. In this case the other Member State may apply the principle of reciprocity.
8. When making a request under paragraph 1(b), the requesting Member State may, where it has a particular reason to do so, also request a transcription of the recording. The requested Member State shall consider such requests in accordance with its national law and procedures.
9. The Member State receiving the information provided under paragraphs 3 and 4 shall keep that information confidential in accordance with its national law.

Article 19 - Interceptions of telecommunications on national territory by the use of service providers
1. Member States shall ensure that systems of telecommunications services operated via a gateway on their territory, which for the lawful interception of the communications of a subject present in another Member State are not directly accessible on the territory of the latter, may be made directly accessible for the lawful interception by that Member State through the intermediary of a designated service provider present on its territory.

2. In the case referred to in paragraph 1, the competent authorities of a Member State shall be entitled, for the purposes of a criminal investigation and in accordance with applicable national law and provided that the subject of the interception is present in that Member State, to carry out the interception through the intermediary of a designated service provider present on its territory without involving the Member State on whose territory the gateway is located.
3. Paragraph 2 shall also apply where the interception is carried out upon a request made pursuant to Article 18(2)(b).
4. Nothing in this Article shall prevent a Member State from making a request to the Member State on whose territory the gateway is located for the lawful interception of telecommunications in accordance with Article 18, in particular where there is no intermediary in the requesting Member State.

Article 20 - Interception of telecommunications without the technical assistance of another Member State
1. Without prejudice to the general principles of international law as well as to the provisions of Article 18(2)(c), the obligations under this Article shall apply to interception orders made or authorised by the competent authority of one Member State in the course of criminal investigations which present the characteristics of being an investigation following the commission of a specific criminal offence, including attempts in so far as they are criminalised under national law, in order to identify and arrest, charge, prosecute or deliver judgment on those responsible.
2. Where for the purpose of a criminal investigation, the interception of telecommunications is authorised by the competent authority of one Member State (the 'intercepting Member State'), and the telecommunication address of the subject specified in the interception order is being used on the territory of another Member State (the 'notified Member State') from which no technical assistance is needed to carry out the interception, the intercepting Member State shall inform the notified Member State of the interception:
(a) prior to the interception in cases where it knows when ordering the interception that the subject is on the territory of the notified Member State;
(b) in other cases, immediately after it becomes aware that the subject of the interception is on the territory of the notified Member State.
3. The information to be notified by the intercepting Member State shall include:
(a) an indication of the authority ordering the interception;
(b) confirmation that a lawful interception order has been issued in connection with a criminal investigation;
(c) information for the purpose of identifying the subject of the interception;
(d) an indication of the criminal conduct under investigation; and
(e) the expected duration of the interception.
4. The following shall apply where a Member State is notified pursuant to paragraphs 2 and 3:
(a) Upon receipt of the information provided under paragraph 3 the competent authority of the notified Member State shall, without delay, and at the latest within 96 hours, reply to the intercepting Member State, with a view to:
(i) allowing the interception to be carried out or to be continued. The notified Member State may make its consent subject to any conditions which would have to be observed in a similar national case;
(ii) requiring the interception not to be carried out or to be terminated where the interception would not be permissible pursuant to the national law of the notified Member State, or for the reasons specified in Article 2 of the European Mutual Assistance Convention. Where the notified Member State imposes such a requirement, it shall give reasons for its decision in writing;
(iii) in cases referred to in point (ii), requiring that any material already intercepted while the subject was on its territory may not be used, or may only be used under conditions which it shall specify. The notified Member State shall inform the intercepting Member State of the reasons justifying the said conditions;
(iv) requiring a short extension, of up to a maximum period of eight days, to the original 96-hour deadline, to be agreed with the intercepting Member State, in order to carry out internal procedures under its national law. The notified Member State shall communicate, in writing, to the intercepting Member State, the conditions which, pursuant to its national law, justify the requested extension of the deadline.

(b) Until a decision has been taken by the notified Member State pursuant to points (i) or (ii) of subparagraph (a), the intercepting Member State:
(i) may continue the interception; and
(ii) may not use the material already intercepted, except:
— if otherwise agreed between the Member States concerned; or
— for taking urgent measures to prevent an immediate and serious threat to public security. The notified Member State shall be informed of any such use and the reasons justifying it.
(c) The notified Member State may request a summary of the facts of the case and any further information necessary to enable it to decide whether interception would be authorised in a similar national case. Such a request does not affect the application of subparagraph (b), unless otherwise agreed between the notified Member State and the intercepting Member State.
(d) The Member States shall take the necessary measures to ensure that a reply can be given within the 96-hour period. To this end they shall designate contact points, on duty twenty-four hours a day, and include them in their statements under Article 24(1)(e).
5. The notified Member State shall keep the information provided under paragraph 3 confidential in accordance with its national law.
6. Where the intercepting Member State is of the opinion that the information to be provided under paragraph 3 is of a particularly sensitive nature, it may be transmitted to the competent authority through a specific authority where that has been agreed on a bilateral basis between the Member States concerned.
7. When giving its notification under Article 27(2), or at any time thereafter, any Member State may declare that it will not be necessary to provide it with information on interceptions as envisaged in this Article.

Article 21 - Responsibility for charges made by telecommunications operators
Costs which are incurred by telecommunications operators or service providers in executing requests pursuant to Article 18 shall be borne by the requesting Member State.

Article 22 - Bilateral arrangements
Nothing in this Title shall preclude any bilateral or multilateral arrangements between Member States for the purpose of facilitating the exploitation of present and future technical possibilities regarding the lawful interception of telecommunications.

TITLE IV

Article 23 - Personal data protection
1. Personal data communicated under this Convention may be used by the Member State to which they have been transferred:
(a) for the purpose of proceedings to which this Convention applies;
(b) for other judicial and administrative proceedings directly related to proceedings referred to under point (a);
(c) for preventing an immediate and serious threat to public security;
(d) for any other purpose, only with the prior consent of the communicating Member State, unless the Member State concerned has obtained the consent of the data subject.
2. This Article shall also apply to personal data not communicated but obtained otherwise under this Convention.
3. In the circumstances of the particular case, the communicating Member State may require the Member State to which the personal data have been transferred to give information on the use made of the data.
4. Where conditions on the use of personal data have been imposed pursuant to Articles 7(2), 18(5)(b), 18(6) or 20(4), these conditions shall prevail. Where no such conditions have been imposed, this Article shall apply.
5. The provisions of Article 13(10) shall take precedence over this Article regarding information obtained under Article 13.

6. This Article does not apply to personal data obtained by a Member State under this Convention and originating from that Member State.
7. Luxembourg may, when signing the Convention, declare that where personal data are communicated by Luxembourg under this Convention to another Member State, the following applies:
Luxembourg may, subject to paragraph 1(c), in the circumstances of a particular case require that unless that Member State concerned has obtained the consent of the data subject, the personal data may only be used for the purposes referred to in paragraph 1(a) and (b) with the prior consent of Luxembourg in respect of proceedings for which Luxembourg could have refused or limited the transmission or use of the personal data in accordance with the provisions of this Convention or the instruments referred to in Article 1. If, in a particular case, Luxembourg refuses to give its consent to a request from a Member State pursuant to the provisions of paragraph 1, it must give reasons for its decision in writing.

Appendix V International Working Group on Data Protection in Telecommunications, Common Position on Public Accountability in relation to Interception of Private Communications

adopted at the 23rd Meeting in Hong Kong SAR, China, 15 April 1998, at http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm

1. While individuals should have a reasonable expectation of being able to communicate in private, other public interests will sometimes justify interception by appropriate authorities.
2. Interception should only be permitted in exceptional circumstances where justified in serious cases and subject to appropriate safeguards - such as judicial authorisation, notification of individuals, limits on use, and requirements for destruction of tapes and transcripts. (This paper does not attempt to deal with these issues, or with interception that may be required for the technical operation of networks or for the purposes of regulatory authorities.)
3. Authorised interception must necessarily be carried out without the prior knowledge of the subjects. However, to confirm with principles of openness, transparency and accountability, there should be mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionally.
Such mechanisms should include:
record-keeping requirements
monitoring and auditing
periodic public reporting.
4. *Record-keeping:* Investigating agencies undertaking interception should keep appropriate records to establish the lawful authority and justification for each interception. Record keeping obligations may also apply to the telecommunications provider involved.
5. *Monitoring and Auditing:* A body independent of the investigating agency should have the role of checking compliance with interception laws, and have the necessary powers, capabilities and resources to undertake inspections.
6. *Public reporting:* Reports should be made publicly available, at reasonable intervals, documenting the scale and characteristics of interception activity, so as to indicate the overall level of intrusion into privacy. Reports may include statistics such as those on:
the numbers of authorised interceptions and their duration
the numbers of applications for interception authority denied
authorisations having special features (such as authorising entry onto private premises) or conditions
the numbers of communications intercepted and of people identified
different methods of interception (such as telephone, fax, e-mail, pager, voice mail)
the general classes of places where interceptions were undertaken (such as business, private homes, cars)
the nature of the offences under investigation
the outcome and effectiveness of interceptions such as cases where no evidence of wrongdoing was found, prosecutions were commenced, transcripts were entered into evidence and convictions were secured
the costs of interception.

7. Information in reports should be presented in a clear and meaningful manner, and should include illustration of trends and significant features of interception activity during the reporting period.

Appendix VI GILC Member Letter on CoE Convention on Cyber-Crime Version 24.2

This letter is available at http://www.gilc.org/privacy/coe-letter-1200.html

This letter has been drafted by Dr. Gus Hosein, Privacy International.

December 12, 2000

Dear Council of Europe Secretary General Walter Schwimmer and COE Committee of Experts on Cyber Crime,

On October 18, 2000 we wrote a letter on behalf of a wide range of civil society organizations to indicate our opposition to the proposed Convention on Cyber-Crime. In that letter we raised our opposition to issues surrounding criminalisation of tools, the issue of liability, sanctions on copyright, enhancing mutual legal assistance, and increased investigative powers. We argued that version 22 of the convention represented the interests of law enforcement, and lacked accountability. As a result, its lack of consideration towards civil liberties was appalling.

To our dismay and alarm, the convention continues to be a document that threatens the rights of the individual while extending the powers of police authorities, creates a low-barrier protection of rights uniformly across borders, and ignores highly-regarded data protection principles.

Although some changes have been made in version 24-2, we remain dissatisfied with the substance of the convention. The convention subcommittee did give our previous letter attention, but we maintain that protections of individual rights have not been attended to adequately. We question the validity of the process that still endures a closed environment and secrecy. As a result, we are following up with this subsequent letter to reiterate our past concerns, address some of the changes, and shed more light on a subset of these concerns.

Exceptions indicate a larger problem

One thematic shift in the convention is the increased number of exceptions and caveats in the current draft. While, these exceptions are still quite weak, it appears as though there is rising concern *within the CoE* as to the powers granted within the convention.

The effect of the deletion of Article 37.2 (from version 22), that once limited the amount of flexibility signatory states are allowed to exercise, appears as though there is an arising opposition among the drafters and plenary member states over this issue.

In Section 2 on Investigative Techniques, article 14.2 was added to assure "adequate protection of human rights and, where applicable, the proportionality of the measures to the nature and circumstances of the offence." While the CoE considered allowing signatory states to restrict the situations for using the new investigatory powers, even from using them in the crimes established in the convention, this was not included in version 24-2. The convention still promotes use of invasive techniques for any crime, except the use of interception, which according to 21.1 can only be used for "serious offences to be determined by domestic law". Even this limitation serves little effect, for the definition of serious crime is left to domestic law, and some countries in the CoE have an extremely broad definition of serious crime for content interception purposes.

An additional exception was appended to Articles 29 and 30, for consistency with a previous article, that a signatory state may refuse mutual assistance to pursue an offence only if the state in question considers the offence to be *political*. Despite that this option existed in another article in version 22, and is consistent with previous CoE documents, it does appear that the CoE is aware of the differences in regimes and qualitative nature of 'offences' in the prospective-signatory states. This exception arises because of the failure to require dual-criminality.

The addition of sub-article 35(bis).4 states that a transferring party *may* require the receiving party to explain the use made of information that is shared between states. This after-the-fact reporting is desirable, but not sufficient. The interests of proportionality and specificity must also be addressed in

requirements applicable to the initial requests for assistance, sufficient to allow the requested party to verify the reason for the investigation by the requesting party.
When a state makes such 'reservations', article 43 contains new sub-articles to place pressure on these states to conform to the full powers of the convention. Subarticle 43.2 claims that signatory states are expected to withdraw reservations "as soon as circumstances permit", while subarticle 43.3 allows the Secretary General to approach these states periodically to discuss the withdrawal of their reservations. The CoE appears to assume that human rights are negotiable, periodically.

Recommendations on Exceptions
We continue to argue that the use of invasive powers must applied only for *serious crimes*.
Proportionality is a concept that must be defined at the international level, uniformly and unilaterally agreed or by reference to the jurisprudence of the European Court of Human Rights.
The current draft's approach of allowing for exceptions and reservations by individual countries is faulty and hazardous to human rights for it fails to set a mutually agreed upon *limit* to the privacy intrusions that will be within the scope of the treaty.
We urge dual criminality as a pre-requisite to all forms of mutual assistance, and these crimes must be stated explicitly.
We also urge the addition of a consistent regime of civil liberties protections in investigative powers.
We urge that the provisions of the draft Convention be consistent with international human rights instruments:
Universal Declaration of Human Rights, article 12, article 19;
International Covenant on Civil and Political Rights, article 17, and article 19;
European Convention on Human Rights, article 8, and article 10.

Influencing Development and Distribution
We also note the addition of a preamble statement regarding the interests in the use and *development* of information technologies. We oppose the creation of a situation where technologies that are proportionate with regards to authentication are dismissed in favour of technologies of full traceability. *We recommend* that this clause be removed.

Powers for Invasiveness
We continue to oppose powers of interception and preservation of data without sufficient constraints.
Article 19.4 continues to allow for self-incrimination by ordering an individual who has knowledge of the security methods applied to the data of interest, to provide all necessary information to enable search and seizure. We remain concerned that this may be a prompt for government access to decryption keys and could breach Article 6 of the European Convention on Human Rights.
Article 20 on access to traffic data fails to acknowledge the invasive qualities of such data, and the shifting division between content and traffic data. Likewise, there is no definition for 'content data'.
The addition of article 20.2 for real-time collection and recording of traffic data through technical means appears to be a prompt to allow for systems such as Carnivore.
The addition of article 21.2 allows similarly for "real-time collection and recording of content data through technical means."
Recommendations on Powers
We urge clear limits to the powers involving situations where civil liberties are compromised. Particularly, we expect that invasive techniques are used only in the case of *serious crimes* and allow for clear prevention of self-incrimination and other inalienable rights, such as privacy and freedom of expression as outlined in the European Convention on Human Rights, the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights.
We view traffic data collection as invasive and urge sufficient uniform constraint prior to collection.
We urge a clear definition of 'content data' and the differentiation with 'traffic data'.
We require *limitations* on the powers of interception and data gathering devices so as to absolutely limit the invasiveness. We recommend that 20.2 and 21.2 are replaced in favour of a protective article ensuring that if technical means are used, these means must separate out the traffic of the specific user under investigation, gather only the legally permitted amount of data, disallow tampering, and respect the shifting division between content and traffic data. If this can not be guaranteed through independent

audit, these techniques must be deemed illegal (similar to Article 3) and no data access or sharing can occur.
Interception of communications is an invasive technique often used against dissidents and human rights workers around the world. We continue to urge you not to establish this requirement in a modern communication network particularly as these networks are still being developed and shaped.
The CoE has stated publicly[a] the difference between retention and preservation of data. However considering discussion at the G8 and recently within the UK[b], we believe that this distinction requires explicit protections. We want to see international respect for data protection as in the 1981 CoE Convention on Data Protection and the EU Data Protection Directive 1995, and apply these instruments to traffic data.
In increasing powers the convention must also establish a maximum threshold of investigative techniques that are acceptable; unjudicious access and data warehousing are gross invasions of civil liberties.

Accession without Rights
It has been stated that the signing of this convention is intended to eventually include non-member states of the Council of Europe. It is our hope that any state that is invited to sign this convention have sufficient respect for human rights and democratic accountability. In particular, these invited states are not signatories to the European Convention on Human Rights and have not necessarily enacted into national law the principles of protection of these rights. As a result, we would consider this invitation to be an attack on the integrity of the convention. *We require* at the very least to see in Article 37 a sufficient requirement and evaluation to the adequacy of human rights protection prior to allowing their accession.

Un-due Extraterritoriality
The convention contains numerous extraterritoriality claims, particularly embodied within two statements.
Article 23 creates supra-national reach for signatory states. Although there is an exception under subarticle 23.2, which the US admits that it will have to pursue[c], as we have stated earlier, if an exception exists, it is often because the measure is too far-reaching.
Footnote 29, which relates to mutual assistance under article 27, specifies "that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party." As a result, signatory states can be forced to act beyond their means.
Recommendations on Extraterritoriality: We find all indications of extraterritoriality to be gross invasions on the sovereignty of nations with respect to the protection of the rights of the individual.
We urge that footnote 29 be withdrawn and the philosophy supporting it be regarded as undemocratic.
We require that states must only be permitted to act in manners for which they have legal, democratically agreed procedure as in the European Convention of Human Rights; otherwise this will allow for the extraterritoriality of extreme powers, such as the UK Government's contentious access to decryption keys under the recently enacted RIP Act 2000.
We recommend a clause be included under mutual assistance that states that when Party A requests assistance from Party B, Party B may not act using powers greater than those allowed for under Party A's jurisdiction, and Party B can only act based on the rule of law within Party B under due process.
We do not want mutual assistance to appear as arbitrage between states where negotiations take place to find increased powers and lowest levels of protections.

Continuing Opposition
We remain concerned with the original objections stated in our October 18 2000 letter; please consider this as a complementary statement of opposition.
We continue to await progress on our previous requirement for judicial review to invasions of privacy. The Council of Europe should clarify these provisions as Section 2 is riddled with access to data without stating a unilateral minimal-level of review and due process. We are also concerned that the convention fails to uphold the privacy rights within the European Convention on Human Rights, to protect them for the digital age. We recommend reference to the Universal Declaration of Human

Rights, particularly article 12 that states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." As a result of its lack of regard to human rights, the convention is currently unsupportable.
The CoE is granting states the terminology and impetus to act against *cyber-crime*; we hope the CoE will take this opportunity to give the signatory states the terminology and impetus to act in the interests of the rights of the individual. Therefore we urge that limits to action be stated explicitly, such as in requiring judicial review, assuring against self-incrimination, ensuring data is gathered for specific reasons, using proportionate means at all occasions, and upholding data protection principles; to name a few.
We continue to believe this convention development process violates requirements of transparency and is at odds with democratic decision making. We only hope that even at this late stage the CoE may learn and practice responsiveness to consultation by incorporating and protecting human rights.
We call on the member-states of the CoE not to sign the treaty in its current format at this time. We also call the Committee of Ministers of the CoE to reject the Convention in its current format in that it does not provide equal protection to fundamental human rights while trying to prevent and detect cybercrimes.
We, the undersigned, continue to make our offer to support the CoE with experts in the area to provide a better version of the convention, aimed not only at punishing, but also at preventing computer crimes and protecting fundamental human rights.

Signed by 22 members of the Global Internet Liberty Campaign

Appendix VII ACLU and Privacy International Model Language for Ratification Letter to National Parliaments in relation to the Cybercrime Convention

This letter has been drafted by Dr. Gus Hosein, Privacy International.

Ratification Letter to National Parliaments

[Date]

Dear [national parliament or government/audience],

We are writing to you as [country] has taken steps towards the implementation into law the measures described in the Council of Europe Cybercrime Convention (ETS 185) [and/or the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems ETS 189] for the purpose of ratification. We urge you to not ratify the convention until the reservations have been considered in full and taken. We have attached to this letter a list of these reservations for your review. We would also like to take this opportunity to offer our comments regarding the nature of the convention, and our specific ideas on its ratification by calling on [country] to preserve human rights as increased criminalisation and surveillance powers are deliberated.

Civil society organisations around the world over a number of years appealed to the Council of Europe (hereafter CoE) for changes and recognition of fundamental human rights. We are now appealing to the [country-ian parliament/government] to try to minimise the damage to civil liberties that may be incurred through implementation and ratification into national law.

Our goal is to see strict definitions negotiated at the national level to counter the ambiguities within the text of the convention; the minimisation of the application of the measures of surveillance; clear processes of authorisation and oversight to the use of invasive surveillance techniques; and the requirement of dual-criminality prior to the use of any of these powers.

What the Council of Europe Convention is...

The CoE cybercrime convention was drafted in relative secrecy from 1997-2000, when it opened a consultation process in April 2000. Few changes were achieved in the consultation stage, however, despite the activities of representatives from industry and civil society. Both industry and civil society organisations opposed loudly the convention on a number of grounds, including the formulation process, invasiveness, costs and burdens, lack of due process provisions, and the presence of ambiguous language within the body of the convention.
The convention was drafted by a group of representatives from national departments of justice and home affairs, most notably Canada, France, Germany, the United Kingdom, and the United States. As a result of the formulation and consultation processes, the convention represents the interests of law enforcement agencies while all but ignoring privacy and civil liberties protections. [*may add that it was of concern to industry as well*]

What the Council of Europe Convention is NOT...
Civil liberties organisations around the world are concerned with the signing and ratification of the Council of Europe Convention on Cybercrime for a number of reasons. These have been summarised in a number of letters and appeals to the drafters of the convention for changes. The CoE responded to these appeals by promising repeatedly that the opportunity for consultation and democratic participation would arise on a case-by-case basis at the national level at the time of signing and ratification.
As [country] prepares to change the domestic legal regime, we would like to take the opportunity to remind [national legislatures] of the actual content of the convention. That is, we offer this reminder of what the convention does not mandate in order to clarify the obligations that are placed upon signatory states.

The Council of Europe convention on cybercrime:
Does not require countries to require lawful access to decryption keys
Does not require countries to allow for interception of communications for all cybercrimes
Does not require real-time access to traffic data for all crimes
Does not require regulation of hate speech and other offensive speech
Does not prevent countries from requiring dual-criminality prior to international co-operation
Does not require powers of traffic data retention
Does not require Internet Service Providers to collect data that they would not normally collect.

Within the convention's ambiguous language and the optional reservations, it is possibly to pursue a ratification process that minimizes the risks and threats to civil liberties and privacy. [*and limits the legal and financial burdens upon industry*]

Recommended Actions
At the ratification stage of the convention a country may pursue a number of reservations that are proposed throughout the convention. At this late stage in the process we would like to remind [audience] of these reservations, and recommend their adoption to minimize the harm to our national interests, while also supporting a strict interpretation of the required changes to domestic law and procedures.

Stricter Definitions -- Article 1
Despite the ambiguous definitions and terminology within the convention, in accordance with Article 1, [country] is not obliged to copy the definitions directly.
Most notably, the task of defining *traffic data* is left to national legislatures. This is a very important definition and it requires substantial negotiation with network service providers, technology providers, and members of civil society due to the costs, availability, and sensitivity of the varying types of transactional data that arise from digital communications and interactions.
We therefore recommend a technology-specific and thorough national dialogue on the [country-ian] definition of traffic data. Even amongst countries with similar legal systems, e.g. Canada, the United Kingdom, and the United States, the definitions already vary greatly.
Ideal definitions must acknowledge that some transactional data can be highly sensitive, including, but not limited to, location data, web sites visited, computer names, chat room conversation data, and

search parameters. While there may be a temptation to define traffic data for the Internet similarly to traffic data for the telephone system, we would warn against such a weak distinction amongst technologies; telephone data is not the same as location data, for example. Once the sensitive data types are noted, lawful access policies of preservation, production, and real-time surveillance should vary according to the data required and produced.
Finally we would like to note that the convention focuses on criminalising and enabling investigations into on-line activities. Therefore the objects of regulation are explicitly service providers for access to computer networks, communications conducted over computer networks, and data in a digital form. The convention must not be seen as an opportunity to criminalise and regulate the conduct in all spheres of life and over all forms of communication infrastructures.

Requiring Intent in Illegal Activities -- Articles 2, 3 and 7
While the criminalisation of 'hacking' activities is among the many goals of the convention, there are still a number of interpretations of what constitutes a 'hacking' event. We recommend that [country], as permitted within Articles 2 and 3 of the convention, require that a hacking event must involve the infringement of security measures with the intent of obtaining computer data or other dishonest intent.
Similarly, countries may require that computer-related forgery crimes (article 7) include the intent to defraud, or similar dishonest intent before criminal liability applies.

Requiring Serious Harm in Interference -- Article 4 and 5
Data and Systems interference may not always involve significant or remarkable damage to the data and systems. The CoE convention acknowledges this within Article 4 by allowing states to reserve the right to require that data interference must, to qualify as a crime, result in serious harm. We recommend that this reservation be pursued by [country] at the time of ratification.
Article 5 already requires that system interference must involve a serious hindering of the functioning of a system. [country] must decide for itself what constitutes a *serious* hindrance. Some suggestions from the CoE include: a requirement for a minimum amount of damage to have occurred, assessing whether the actions involved a partial or total hindering, temporary or permanent.

Reduced Criminalisation -- Article 6
The convention appears to require the criminalisation of the *possession, production, sale, procurement for use, import, distribution or otherwise making available* of devices and similar data with the intent for use in hacking activity. The very same article, article 6, acknowledges that criminalising the *procurement for use, import, possession* is not a necessary imposition.
As some of these devices and similar data have multiple uses, some positive others negative, we recommend therefore that the procurement, import, and possession not be criminalised.

Strictly Defining 'Intent' and 'Without Right' -- Articles 2, 5, 6, 7, 8, and 9
When discussing hacking crimes, the terms 'intent' and 'without right' are repeatedly used to qualify the constitution of a crime. The convention does not actively recommend a definition for these key terms, however. The discussion of these terms in detail occurs in the Explanatory Report of the convention.
Countries are generally expected to criminalise activities conducted *intentionally*. The Explanatory Report expands upon 'intent' claiming that it may require 'knowledge and control' of the activities occurring (in the case of hacking activities), or information that is transmitted and stored (in the case of child pornography and illegal devices), or the goal of the action was to gain economic benefit (for computer-related fraud). The CoE argues for an appropriate definition of sufficient intent, so that service providers that served as conduits or hosted content are not held criminally liable for conduct and content. Similarly, there is no requirement for service providers to monitor the conduct of its clients to avoid liability.
'Without right' is a flexible term in that [country] is permitted to take into account fundamental rights, such as freedom of thought, expression and privacy as it is adapted to national law. This situation is likely to arise in the arts and sciences, possibly creating chilling effects upon these disciplines. The Explanatory Report is also concerned that 'legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised'.
We therefore call for a detailed national dialogue regarding the terms 'intent' and 'without right'.

Limiting Criminal Liability, Offences, and Sanctions -- Articles 10, 11, 12 and 13
The article establishing the offence of infringement of copyrights and related acts, Article 10, may be redundant considering existing international obligations, presuming that a country is already bound by these other treaties and conventions. Even if a country is not already bound by these obligations, there is no requirement that states proceed to be bound by the cybercrime convention.
The convention allows national governments to decide for themselves the precise manner in which such infringements are defined under domestic law. Therefore, [country] is within its right to impose criminal liability in a way of its own choosing. We therefore recommend a national dialogue on this issue.
Similarly, a reservation is allowed under the Article 11 offences of attempt, aiding or abetting a crime. To be specific, a reservation may be pursued to limit the liability of those who attempt certain crimes, particularly hacking activities, forgery and fraud, production and distribution of child pornography (Articles 3-5,7,8,9(1)(a) and 9(1)(c)). As a result, [country] is under no obligation to criminalize the 'attempt' of an activity. We recommend that [country] pursue this reservation to limit the liability on third parties, and to further the goal of strictly-defining 'intent'.
Finally, the sanctions against all the crimes discussed above, according to the convention, are to be decided by national governments. A thorough national dialogue of appropriate sanctions is recommended.

Limiting the Scope of Application of Real-Time Surveillance -- Article 14, 20, 21
The CoE convention acknowledges that real-time surveillance of communications and traffic data are invasive procedures. In the case of the interception of communications content data in Article 21, the convention requires that national parliaments establish a range of *serious offences* in which an investigation may occur using this invasive power.
Similarly, the real-time collection of traffic data may also be limited to a range of crimes, according to Article 14, so long as the range is not more restricted than the range of serious offences for interception. Accordingly, we recommend that real-time collection of traffic data, provided for under Article 20, is also limited in use only for serious offences, and not necessarily including the hacking activities and other crimes established within the convention.
The convention also acknowledges that these powers do not need to apply to all telecommunications systems. Particularly, Article 14 allows for the exclusion of service providers for closed groups of users and that do not employ public communications networks. We would like to suggest an extension of this exclusion principle, and allow for a national dialogue on which service providers do and do not need to comply with real-time surveillance requests and associated financial and operational burdens. We would recommend against imposing these costly burdens upon public service providers such as libraries, schools, and universities, for example.
We believe that limiting specifically the scope of application of these powers, and the other powers discussed in detail below is essential for the preservation of human rights within [country]'s democratic legal system. This is consistent with other international conventions and practices, including the European Convention on Human Rights and associated jurisprudence, the United Nations Declaration of Human Rights[, and other such constitutional or legal provisions at the state level].

Assuring that Implementation is Consistent with Domestic and International Legal Protections of Rights -- Article 15
The convention, in Article 15, requires that countries ensure that the powers and procedures implemented in accordance with the convention are subject to conditions and safeguards in national law to provide for the adequate protection of human rights and liberties. This includes incorporating the principles of specificity, proportionality; ensuring adequate judicial supervision; assuring due process is followed through such measures as providing sufficient grounds prior to applying the powers; and limiting the scope and duration of these powers.
We therefore recommend that [country] conduct an open dialogue of the invasiveness of all of these procedures and regarding the need to update and enhance human rights protections in the light of new technological developments. Different technological infrastructures involve different impacts on rights, responsibilities and legitimate interests of third parties. The convention calls for countries to consider

these issues, in Article 15.3. While [country] considers powers of surveillance for new technologies, we must also consider the rights of individuals.
We also recommend that, in accordance with the requirements of the CoE convention, judicial authorisation is required for invasive surveillance, complemented by adequate and sufficient oversight, reporting, and notice of all activities.

Specificity and Limitation in the Expedited Preservation of Data -- Articles 16 and 17
Expedited action by law enforcement authorities to order the preservation of data is an onerous and burdensome obligation to place upon third parties. We would like to note that preservation, according to the Explanatory Report, applies only to existing data and does not require service providers to store data that is not otherwise collected. Nor is it necessary for the preserved data to be rendered inaccessible; and the data needs to be preserved only for a maximum period of 90 days. We expect that orders will go through appropriate authorisation and oversight channels, as required by Article 15.
The partial disclosure orders in article 17 are problematic because of the expediency requirement. We are deeply concerned with this power, and would like to ensure that it is used in limited and specific circumstances. In accordance with advice from the CoE, we also recommend that the authorities requesting partial disclosure "should specify clearly the type of traffic data that is required to be disclosed".
We also recommend that in accordance with Article 15, the type of data be minimised to meet only its purpose of identifying the next point in the chain of communication and not any further information regarding the nature and content of the communication. This further information should instead be accessed using other powers and more thorough procedures.

Specificity in Production Orders -- Article 18
While the convention, under article 18, requires national parliaments to empower authorities to order the production of information, the CoE notes that the order may not necessarily require the production of all data in a person's possession or control. Different forms of production orders may be prescribed by national parliaments according to the type of information being disclosed.
We therefore recommend that a national dialogue occur regarding each type of information that may be produced under these orders and the required authorisation and oversight, in accordance with Article 15 of the convention. This dialogue should also consider the way in which the sensitivity of information varies depending on the technology and the context of its use. As examples, traffic data differs according to the type of service used; subscriber records may contain sensitive information depending on the type of provider; particular data may contain personally identifiable information of individuals other than the suspect.
We also note that the convention does not require a change in the practices of service providers. Preservation and production orders may not force service providers to collect data that is not normally collected in the process of doing business. This is particularly important to note for the production of traffic data and subscriber records: if this information is not already collected by service providers, the convention does not require a change in this practice. Additionally, service providers are not expected to implement measures to ensure the integrity of the data if it is collected. Finally, the CoE notes that in accordance with Article 15, judicial authorisation may be required, and the amount of data solicited must be minimised to prevent data-mining.

Specifying the Search and Seizure of Stored Data -- Article 19
The convention requires countries to adopt measures measures to allow for the search and seizure of stored data. This power does not require the collection of a specific form or type of data, it only requires that if the data exists, government agencies may search and seize the information.
The CoE notes that there is some confusion in the case of electronic mails (e-mails) stored on the servers of service providers. The CoE accepts that countries may and do regard this data as 'communications' and not as stored data, therefore requiring greater authorisation and oversight and more limited use of this power. We therefore recommend that [country] clear this confusion through the establishment of legal protection to stored communications, regardless of having been read by the intended recipient, to the same degree as communications in-transit.

Another source of confusion surrounds the situation where the data requested is protected or secure. In an ambiguous article 19.4, the convention calls on governments to allow for access to secured and protected data by requiring those with a knowledge of the functioning or measures applied to assist in enabling lawful access. The convention is very clear, however, that this forced disclosure must be necessary and reasonable. In accordance with articles 14 and 15, 'reasonable' means specific, proportionate, and necessary; while consistent with international and national human rights instruments, and other such legal principles. Therefore this power can not be designed to conflict with rights preventing forced self-incrimination, while also limiting the disclosure of sensitive information held by third parties.

Limiting Jurisdiction -- Article 22

Acknowledging the international nature of communications networks, the convention endeavours to establish jurisdiction over the activities of individuals. The only requirement within the convention, however, is that jurisdiction may be established within the territory of the state. Countries may therefore use a reservation to not apply jurisdiction globally just because the alleged offence involves the investigations of one of its nationals[*, or on board a ship and aircraft registered under its laws*].

We therefore recommend that [country] pursue the reservation to limit jurisdiction to its national territory.

Restricting Compelled International Co-operation -- Articles 23, 24, 28

While the convention appears to, under article 23, to require the co-operation amongst states in the investigation of criminal offences and for the collection of evidence, there are a number of grounds for refusal and reservations that [country] may pursue.

In the case of extradition as under Article 24, [country] may refuse to extradite an individual if it is not satisfied that all of the terms and conditions of the extradition are adequate.

In accordance with Article 28, the requested party may restrict co-operation through the sharing of investigative data on the requirement that it not be used for investigations or proceedings other than those stated in the request.

Finally, [country] may refuse requests for co-operation, within articles 27.4, 29.5, and 30.2, if [country] believes that the offence being investigated is a political offence or connected with a political offence, or prejudicial to [country-ian] sovereignty, ordre public or other essential interests. We believe it is important for a national dialogue on what qualifies as a 'political offence', 'ordre public', and 'essential interests', and the procedures through which such qualifications are deliberated on a case by case basis. We believe that the protection of the rights of individuals within [country] are an essential interest to [country], that can not be departed from, as in the sense of ordre public. We also contend that any individual exercising their political rights should be protected by the 'political offence' clause.

In fact we would like to see increased openness in the negotiation and conduct of international co-operation. There is a growing emphasis on international co-operation, and we believe the time is now ripe for a national dialogue on such issues as grounds for refusals, national conditions upon co-operation, adequate oversight and reporting mechanisms. We would like to see a yearly account reporting on the substance of investigations where [country-ian] agencies were called on to co-operate with another country in criminal investigations.

Requiring Dual Criminality

The basis for international co-operation within the convention in Article 23 is that there must be a criminal offence being investigated. Meanwhile, in accordance with Article 25.4 all co-operation is governed by national law of the requested country. Therefore, dual criminality requirements flow naturally: [country] may only respond to requests for investigative data regarding an offence, in accordance with [country-ian] law, according to procedures established in [country-ian] law.

In all cases of international co-operation, [country] may require dual-criminality. In implementing the convention into national law, we recommend that this requirement be made explicit in order to be compliant with Articles 14 and 15 of the cybercrime convention, that require proportionality, specificity, and sufficient authorisation and oversight. [country]'s government agencies must not apply investigative powers and share investigative data if the conduct to be investigated is not illegal within [country].

In other words, [country] must not be required by other countries to use powers that are not on a statutory basis, therefore forcing [country]'s agencies to break [country]'s own laws.
The convention appears to limit the requirement of dual-criminality for expedited preservation of stored data, under article 29. In this case, [country] has to actively reserve the right to refuse the request on the grounds of requiring dual-criminality, and may do so if [country] law refuses to order the production of data unless an investigation is occurring into a specific crime, according to [country-ian] law. Expedited preservation of data places burdens on service providers as well as individuals; particularly if it is not for pursuing a crime according to [country]'s criminal justice system. We therefore recommend that at the time of ratification, the [country]'s parliament declare to the CoE the intention to refuse requests for expedited preservations unless dual-criminality can be verified at the time of the request.
We also recommend an adequate reporting scheme be established to monitor these developments.
Concluding notes
It is a positive sign that the convention text allows for the flexibility outlined above. It is not a positive sign, however, that these are merely allowances to national parliaments rather than being strictly required by the convention. Therefore, national debate is essential and necessary to the successful integration of the convention into [country-ian] law.

We, the below signed organisations call on [country]'s parliament to ensure that the Council of Europe cybercrime convention does not improperly extend the powers of the state in such a way that contravenes our own legal regime, international law, and the protection of the rights of the individual.
We look forward to future dialogues regarding this important convention and the important legislation being considered.

Signed