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

Preface

The Council of Europe is preparing a "Convention on Cyber-crime" which intends "to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offence". Major non-European countries, such as the United States, Canada, Japan and South Africa are participating in the drafting process. The draft Convention is expected to be finalised by December 2000 and to be open for signatures as early as September 2001. The draft itself allows for accession of any other state at the invitation of the Committee of Ministers. The Council of Europe has stated that it seeks to enhance the consultation process with interested parties, whether public or private.

The Working Group acknowledges that there is a need to fight international computer-related crime, that enhanced international co-operation is needed in the era of global communications networks and that law enforcement authorities need appropriate means for fighting such crimes. On the other hand such measures have to be balanced with other common values, e.g. the right to privacy and to telecommunications secrecy.

Whereas the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union expressly regulates the protection of personal data (Art. 23) the present draft convention on cyber-crime does not contain any reference to privacy regulations. It fails to outlaw infringements in a clear and unambiguous way on personal privacy by the mere access to computer systems.

The Council of Europe has a longstanding tradition of developing data protection standards on a multilateral basis. It seems therefore appropriate that the new convention expressly refers to Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981 and Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services. The Working Group considers it necessary that the Committee of Experts on Data Protection is included in the further drafting process.

New Procedures

The Convention on cyber-crime intends to introduce new procedures to allow for the prosecution of crimes related to the Internet use, including measures to compel telecommunications service providers to store personal data (both content and traffic data) of communications via telecommunications networks and to make these data available to the national and foreign authorities engaged in criminal investigations and proceedings.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

There has been discussion in the past in different contexts on obliging telecommunications and Internet Service providers to store data on all telecommunications and Internet traffic for extended periods to have the data at hand if a crime occurs in this period. The Working Group deems such measures as disproportionate and therefore unacceptable. The Working Group underlines that traffic data are protected by the principle of confidentiality to the same extent as content data (Article 8 of the European Convention on Human Rights). In this respect the Working Group fully supports the findings of the European Data Protection Commissioners Conference at its meeting on 6/7 April 2000 in Stockholm where the Conference has stated that such retention of traffic data by Internet service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights (http://www.datenschutz-berlin.de/doc/eu/konf/00_db_en.htm; cf. also Recommendation 3/99 of the Article 29 Working Party on the preservation of traffic data by Internet Service Providers for law enforcement purposes; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp25en.pdf). This goes also for storing data revealing the use of the Internet by individuals.

Existing powers for tracing crimes should not be extended in a way that invades privacy until the need for such measures has been clearly demonstrated.

The Working Group has in the past stated that any Interception of Private Communications should be subject to appropriate safeguards (cf. Common Position on Public Accountability in relation to Interception of Private Communications; adopted at the 23rd Meeting in Hong Kong SAR, China on 15 April 1998; http://www.datenschutz-berlin.de/attachments/174/inter_en.htm). Existing conditions and safeguards provided for under domestic law and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (Art. 23) must be respected. Such conditions and safeguards should at least include

- prior judicial authorisation,
- (subsequent) notification of individuals,
- limits on use,
- record-keeping requirements,
- monitoring and auditing as well as
- public reporting.

Accordingly such safeguards should also be incorporated in the draft Convention on cyber-crime. In particular the cooperation of national authorities with operators of public and private networks should be based on solid, legal obligations rather than on voluntary agreement that are very difficult to control.

New offences

At the same time the Convention intends that several new offences which have not been incorporated in the criminal laws of many member states of the Council of Europe may be introduced.

The introduction of new offences in the criminal law has to be handled extremely carefully, as a broad wording of such new offences as well as the penalisation of attempt and aiding and abetting such offences might lead to a considerable lowering of the privacy standard for all users of telecommunications networks by producing an enormous amount of personal identifiable data about Internet and telecommunications network usage, thus abolishing the right to anonymous use of such services. It is to be foreseen that the envisaged regulations might lead to a need to personalise

every single action of every single user in the global network, which would clearly be disproportionate.

Regarding the offences that are dealt with in Articles 1-13, especially the criminalization of "Illegal devices" (Article 6), "Data Interference" and "System Interference" (Articles 4 and 5) the Working Group takes the view that obligations on the parties to the Convention to compel service providers to take certain security measures when connecting their systems to a public network in order to enhance the security standard on the Internet in general would be more suitable for fighting cybercrime than simply creating new offences, which relate to a wide scope of internet activities and could even penalise activities which are intended to improve security of the network.