BERLIN RESOLUTION OF THE INTERNATIONAL CONFERENCE OF DATA PROTECTION COMMISSIONERS OF 30 AUGUST 1989

World-wide telecommunications are evolving rapidly. International data networks are increasingly used for transfers of personal data, for instance in the use of credit cards, for the purposes of travel booking systems and within multinational enterprises. The use of this new technology can bring significant benefits. But it also increases the problem of safeguarding the position of those individuals whose details are transmitted around the world.

The Council of Europe, the OECD, the United Nations and other international organisations have adopted recommendations and guidelines on data protection. A common feature is a set of principles of good practice such as those in the Council of Europe Convention (Treaty 108) and in the OECD guidelines. These good practices are designed to safeguard the privacy of individuals.

So far, eight states have acceded to the Council of Europe Convention and so committed themselves internationally to legally established data protection standards. Data protection authorities in those countries have some authority to control the transborder flow of personal data when this is necessary to protect individuals. However, controlling transborder data flows in this way presents severe practical problems. In most cases, therefore, data transmissions across national borders implies that the individual can no longer ensure that the principles laid down by national laws and the various international agreements will be applied to his or her data.

For example there can be no guarantee that the data is up to date, accurate, and used only for proper purposes; and the individual loses the opportunity to appeal to any data protection commissioner.

The solution to giving effective international protection to personal data lies in equivalent legal safeguards in the transmitting and receiving countries. This solution is consistent with the international recommendations and guidelines referred to above.

The Data Protection Commissioners believe that data protection should be given the same priority as the promotion of data processing and telecommunications in the development and use of international data services. They therefore recommend that:

- Governments should move rapidly both individually and through international bodies towards establishing equivalent legal safeguards as soon as possible.

- Those transmitting personal data across national boundaries should check and monitor the protection given to such data by those receiving them, with a view to ensuring that proper regard will be given to the position of individuals.

The objective of these actions should be to ensure that:

- The Basic Principles for Data Protection contained in Treaty 108 and in the OECD guidelines are guaranteed to an individual notwithstanding the transfer of his data across national boundaries.

- On a growing scale, personal information data bases are maintained by the European Community institutions themselves. However, these institutions are not subject to data protection legislation and hence to any requirement to meet the Basic Principles for Data Protection.

The European Community and its member nations are therefore urged to take full account, in their planning for "Europe 1992", of the need for a complete and consistent approach to implementation of the Basic Principles for Data Protection across community nations and within community activities.

The detailed proposals put forward by the European Community Commissioners are as follows:

* Appropriate legal instruments should ensure that the Basic Principles of Data Protection contained in the Council of Europe Convention (Treaty 108) will be binding on all member nations and on the EC institutions themselves;

* An independent data protection authority should be established to advise the EC institutions on all data protection issues and to supervise the processing of personal data within these institutions. It should consider complaints from individual data subjects and co-operate with the national data protection bodies.

The Commission Nationale de l'Informatique et des Libertés (the French Data Protection Commission) is invited to submit these proposals to the Presidents of the Council of Ministers, of the European Parliament and of the EC Commission as soon as possible and to try to gain their support.

ADDITIONAL STATEMENT BY THE DATA PROTECTION COMMISSIONERS OF THE EUROPEAN COMMUNITY (EC) NATIONS

The Data Protection Commissioners of the European Community Nations believe that the existence and the activities of the Community give rise both to particular requirements for data protection and to increased opportunities for making data protection effective across national boundaries.

- The EC internal market to be achieved by the end of 1992 is oriented towards the free exchange of information, including personal information, for instance in the

fields of direct marketing/address trading and credit reporting.

- European Community decisions increasingly call for the collection and processing of personal data to be carried out by member nations, for instance in the field of agricultural statistics. They also call for transborder data transmission, for instance in the environmental, health-care and social fields.

- Some Community nations are already working on a pilot project to establish common police "wanted persons" files (the Schengen Information System) to provide a substitute, as it were, where controls at international frontiers are to be abolished.

- Internationally operated data processing systems are structured in such a way that the individual can safeguard his data protection rights without undue difficulty.

- Any correction, up-dating and erasure applied to data which has previously been transmitted abroad will also be applied to the transferred data in any foreign country concerned.

- The greater risks entailed by international exchanges of data to the rights of individuals to decide on the use to be made of their data, are counterbalanced by international co-operation among data protection commissioners.

RESOLUTION OF THE ELEVENTH INTERNATIONAL CONFERENCE OF DATA PROTECTION COMMISSIONERS ABOUT THE WORKING GROUP ON "MEDIA"

August 30th 1989

When drafting the resolution on ISDN the delegation had a first, fruitful exchange of information.

- When we express opinions or make decisions on our countries, we have to take into account the international dimension of telecommunication networks and services.

- Information on events taking place beyond our national borders can not be provided to us by our national operators only.

- Networks and services do not always develop at the same time and at the same place in our countries.

- Experience has shown that the efficiency of data

protection in this field depends - beyond mere principles - on practical measures, and this is not always easy to obtain from our national operators.

This is why the Conference agrees that this Working Group should continue its work in Berlin. Each delegation should have the opportunity to present its experiences in detail (analysis of the problems, possible solutions, adopted solutions) particularly in the following fields:

* detailed bills
* provisions regarding the listing of subsribers in directories and the use of directories
* the different categories of telematic services (electronic mail, teleshopping, information services)
* telemetry
* ISDN
* cellular telephones (digital car telephone)
* automatic prerecorded message devices
* network security

RESOLUTION OF THE INTERNATIONAL CONFERENCE OF DATA PROTECTION COMMISSIONERS ON INTEGRATED SERVICES DIGITAL NETWORKS (ISDNs) OF AUGUST 30TH 1989 PROPOSED BY THE WORKING GROUP ON MEDIA

The present national and international development of telecommunications is characterised by the introduction of Integrated Services Digital Networks (ISDNs). These provide multiple services.

This development means that considerably more personal data is processed by network operators as well as by service suppliers than was the case with previous networks. This development calls for national and international measures to ensure the protection of personal data.

The International Conference of Data Protection Commissioners believes that considerable efforts are required in the light of this development. In particular, not only should data protection not be seen as an obstacle to the development of the international information market. On the contrary, it represents a necessary complement to the technical development, one which is essential to the acceptance of the new telecommunications technologies - it may even be an element that will accelerate this development.

In the case of open networks, data protection should be based on the following principles:

- Accounting data should be stored only if, and only for as long as it is essential for drawing up bills or responding to disputes about accuracy. Furthermore, itemised bills should be provided solely for those subscribers who request them.

- Anonymous payment procedures should be established for certain telecommunications services (telephone, cable TV with feedback channel, data transfer services, motorway toll etc.). Despite billing problems, the multi-purpose character of the networks makes it necessary for them to be provided with the technical potential for anonymous access.

- Data necessary for establishing a circuit should be deleted immediately. Other data may be stored only if it is essential for carrying out a service.

- Precautions have to be taken so as to ensure that those subscribers who want to be recorded in directories will not be subjected to undesired commercial advertising. The right to deletion without charge from subscriber directories should be an objective. Data collected and stored so that subscribers can be reached must not be used to draw-up subscriber profiles allowing behaviour to be monitored.

- Data protection measures, in particular to prevent unauthorised access, manipulation and interception, and those to authenticate the identity of the originator of a message, must be provided to the highest possible technical standards and at an acceptable cost.

- Adequate regulatory institutions should be set up on both a national and international level.

- In the case of Local Area Networks and telecommunication terminals, data protection must initially be taken into account at the stages of setting design standards and approving equipment.

The following service features require particular attention:

- It must be possible for the identity of the caller to be suppressed by either the caller or the person being called. Abuse must be forestalled by provisions in the network.

- Installations for on-hook operating must be designed in such a way to guarantee that neither interception nor recording is possible without the concerned parties knowing about it.

- Access to answering machines, voice and mailbox systems must be adequately secured.