Explanatory Memorandum
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

Introduction

1. The work of the Council of Europe in the field of data protection has always endeavoured to be technologically relevant. For example, the drafters of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 footnote 1 deliberately avoided making it rigid by going into detail. The generality of the Data Protection Convention's principles thus allows it to evolve over time. Moreover, the sectoral recommendations so far adopted by the Committee of Ministers, and to which reference has been made in the introduction, have invariably sought to address new problems in a technologically relevant manner.

2. In a similar vein, the members of the Project Group on Data Protection, the drafters of these legal instruments, have now turned their attention in this recommendation to the sector of telecommunications and in particular telephony. The risks which developments in telecommunications bring for private life have already formed the basis of a report which was drawn up by the project group and subsequently approved for publication by the Committee of Ministers footnote 2. Building on some of the themes set out in that report, the project group has sought in this recommendation to provide a number of guiding principles to guarantee the privacy of the individual in his use of telecommunication services and in particular new telephone services. Once again the approach of the group is intended to be technologically relevant.

3. While seeking to address some of the traditional problems which have long characterised the use of the telephone since its introduction, for example the vulnerability of telephone communications to unauthorised interference or interception, the principles contained in the recommendation deal primarily with the new issues which are being created as a result of the digitalisation of networks and the new services which this development has ushered in.

4. These developments of course offer enormous advantages to subscribers and users in general. The availability of detailed invoices brings with it advantages for consumers - they have a greater control over their spending through being able to see from the bill how to use the telephone more economically. In addition, calling-line identification is an effective means of combating malicious or abusive callers. A final example of new development is mobile telephones, which allow businessmen on the move to stay in touch with their offices.

5. It is, however, necessary to weigh these advantages against the costs to protection of privacy. The project group has noted a number of these features which require careful reflection at the level of data protection so as to ensure that the right legal environment exists for their introduction and use. In particular, the committee of experts is conscious of the fact that certain of these new services (for example, calling-line identification) generate personal

data when used, while the digitalisation of networks in general will result in the greater storage of service data by network operators (as illustrated by the availability of detailed invoices). For the project group, these aspects of development may not only threaten the privacy of subscribers and users in general, they may also inhibit their freedom of communication since they diminish the degree of anonymity which subscribers and users may wish to avail of when using the telephone by obliging them to reveal their identities or to leave behind electronic traces which allow their use of the telephone to be monitored.

6. The broad principles contained in the Data Protection Convention apply, of course, to the collection and processing of personal data by network operators and providers of telecommunication services in both the public and private sectors. Nevertheless, it has been felt appropriate to offer specific rules and guidelines for this sector based on the convention's principles, taking account of the sector's specific characteristics, including the characteristics of the new developments referred to earlier. For example, it is not immediately obvious how to find solutions to the new problems raised by calling-line identification from a reading of the convention. Appropriate solutions to the new problems can be found only on the basis of an exhaustive analysis of the sector. Only then is it possible to determine the concrete meaning of the Data Protection Convention's principles of "fair and lawful collection" or "purpose specification" or "data security", and so on.

7. Moreover, it will be seen that the approach of the drafters of the recommendation is underpinned by other fundamental norms in addition to those laid down in the convention. The approach followed in the recommendation refers frequently to Article 8 of the European Convention on Human Rights and to the relevant case-law of that convention's organs. Of particular significance is the assimilation of personal data processed by network operators in the course of or following the use of a telecommunication or telephone service with the principle of secrecy of correspondence guaranteed by Article 8.

8. Finally, one of the broad principles contained in the Data Protection Convention concerns the equivalent protection of personal data which are transferred across national borders. It is clear that the developments in telecommunications lead to an increased international communication of personal data.

In the light of the complicated nature of the issue and the many problems which would be raised by any attempt to regulate, at this stage, transborder data flows in the telecommunication sector, the drafters agreed not to address the issue in this recommendation.

Preamble and operative part

9. The principles contained in the recommendation are addressed to a number of parties.

10. In the first place, the governments of the member states are recommended to reflect the principles in their domestic law and practice. Data protection legislation is an obvious vehicle for expressing the principles, in particular through its implementation by the authorities established under such legislation. This is why the Committee of Ministers has recommended that the recommendation be brought to their attention. Data protection authorities may find solutions to problems which they encounter in this sector contained in the recommendation. After all, this legal instrument has been drawn up by a specialist committee at the international level in the light of comparative analysis of the problems and appropriate ways of dealing with

such problems. Acceptance of the various approaches set out in the recommendation also contributes to realising "the greater unity among the member states of the Council of Europe" in the area of data protection.

11. As the operative part of the recommendation recognises, data protection legislation is not the only legislative form for reflecting the recommendation's principles. Telecommunication laws may also perform this function. Indeed, the trend towards sectoral regulation of data protection issues in many countries would suggest that this would be a better course of action, given the inability of general data protection laws to provide detailed rules for all private and public processing contexts. It should be pointed out, however, that regardless of the choice of legislative form used to reflect the principles, the competence of the data protection authorities to deal with problems arising in this sector remains unchanged.

12. The reference in the operative part to "domestic law and practice" allows for additional flexibility in the implementation of the principles contained in the recommendation. For example, the principles could be embodied in the agreements between governments and network operators which grant concessions to the latter to provide and operate a telecommunication network. Codes of practice may be drawn up within the representative bodies of the sector concerned so as to ensure that the principles are respected in practice within the industry. However, care should be taken to ensure that such codes receive the approval of a superior authority, for example a data protection authority, or a regulatory agency in the telecommunication sector.

13. Moreover, the text also recommends that the principles be communicated to a number of key actors in this sector. The reference to equipment and software suppliers is to be explained by the fact that the principles encourage the exploitation of hardware and software so as to promote technical ways of minimising the storage of personal data at the time of using a telecommunication service, including a telephone service. In particular, suppliers of hardware and software should avoid bringing on to the market and exploiting commercially, gadgets or accessories to the telephone which are prejudicial to the privacy of third parties.

14. The reference to consumer organisations is explained by the fact that telephone subscribers are often mobilised in groups which have to be consulted by network operators. The principles contained in this recommendation have quite obvious consumer impact. Such groups should endeavour to impress on network operators the importance of giving effect to the principles.

15. Finally, a number of international bodies are competent in various aspects of telecommunication policy. Standardisation is frequently determined at the international level. The European Commission has recently produced its own set of draft proposals for ensuring privacy in telecommunication networks within the European Community states. Given the special competence of the Council of Europe in the field of data protection, it is felt appropriate to remind such fora of the importance and relevance of this recommendation.

Appendix to the recommendation

I. Scope and definitions

16. In accordance with Principle 1.1, the scope of the recommendation includes network operators and service providers in both the public and private sectors as well as other public or

private bodies offering networks and/or providing telecommunication services which allow for correspondence or communication between users.

17. In accordance with the Data Protection Convention, the principles contained in the recommendation are directed primarily at personal data undergoing automatic data processing, while allowing member states the possibility to extend the principles so as to include personal data undergoing manual processing (Principle 1.2). It is to be noted that certain European laws on data protection cover both forms of data processing.

18. Again, following the example of the Data Protection Convention, member states also have the possibility to include legal persons within the scope of the recommendation and to extend the principles to the collection and processing of data relating to corporate bodies, associations, and so on (Principle 1.3). As with manual data processing, certain countries in Europe include within their data protection laws both legal and natural persons.

19. The definition of "personal data" in Principle 1.4 has already been used in many of the sectoral recommendations adopted by the Committee of Ministers in the field of data protection. Once again, the definition is in conformity with the Data Protection Convention. It goes without saying that a telephone number is personal data for the purposes of this recommendation.

20. As noted earlier, the digitalisation of networks has brought about a situation in which the same telecommunication line and network may be used for the transmission of voice, text, image and data. In Europe, there is a move towards what is called the Integrated Services Digital Network (ISDN). The digitalisation of networks has led the drafters of the recommendation to avoid over-concentration on telephony in the classical sense of voice communication between users of a telephone. Limiting the approach to voice communication would result in overlooking such matters as text or image transmission via facsimile. Accordingly, the recommendation is concerned with all those facilities which telecommunications now offers to allow users to communicate or correspond inter se. The definition of telecommunication services might even include such matters as interactive videotex, or telemetry, or electronic consultation of data bases, which raise similar problems and should be treated similarly. Radio broadcasting and television are, however, not included in this definition.

21. The network operator is defined in Principle 1.4 as the public or private body which makes available the network so as to allow subscribers and users in general to correspond and communicate by one of the various services mentioned in the preceding paragraph. The network operator's primary function is limited to the provision and functioning of the network, with the services being made available by "a service provider". If the network operator provides services in addition to making available and ensuring the functioning of the network, the specific provisions for service providers apply also to him.

22. The text recognises that "service providers" may also operate their own private networks for communication and correspondence by voice, image, text and data transmission. Alternatively, these services may be provided through the main networks offered by network operators. The text of the recommendation seeks therefore to embrace both network operators

and service providers in so far as they collect and process personal data for the purposes of providing and operating a telecommunication network or telecommunication services.

23. The drafters of the recommendation did not think it necessary to define the term "telecommunication network", and referred to the definition in other relevant international texts.

24. Without wishing to define the term in the recommendation, the drafters agreed that the word "users" would refer to the end users of telecommunication services, including, as the case may be, other network operators and service providers. Similarly, they agreed that the expression "subscriber" would refer to any person who has concluded with the network operator a contract to supply telecommunication services with a view to making use of these services.

25. The recommendation does not use the terms "basic data" or "content data", which within the industry are taken to refer to subscriber data and the content of communications respectively. The text seeks to avoid overly technical language so as to make it readily understandable. Likewise the drafters avoided, in Principle 4.5, using the expression "service data". They agreed, that the term "service data" should embrace the totality of personal data generated through use of a telecommunication service and stored by the network operator for technical and operational purposes, including prevention of abuse, as well as for invoicing purposes.

II. Respect for privacy

26. In addition to respect for privacy, Principle 2.1 advocates that developments in the telecommunication sector should not inhibit freedom of communication. The drafters agreed that this principle would apply to both users and their correspondents. As will be seen at a later stage, telephone services such as calling-line identification as well as the provision of detailed invoices may deter subscribers or users from communicating by telephone since they tend to undermine anonymity. Various provisions in the recommendation seek to minimise these problems which may accompany the disclosure of personal data at the time of making telephone calls. In addition, Principle 2.2 seeks to encourage network operators, service providers and equipment and software suppliers to try and come up with ways of developing anonymous means of access to telecommunication networks. For example, it may be possible to introduce a system based on the pre-paid telephone cards which are used in public telephone booths. This recommended course of action aimed at increasing anonymity is part of a more general theme, namely the need to exploit information technology so as to limit the amount of personal data which are collected and processed as a result of the use of the telephone or of telecommunication services in general. Principle 2.2 is based on the assumption that if the introduction and use of information technology, and in particular the digitalisation of networks, has increased the quantity of personal data which are collected and stored, then it must also be able to minimise personal data storage through the development of "privacy friendly" technology. One aspect of this will be discussed in the context of Principle 7.16, namely the need to develop techniques for suppressing the display of the telephone number of an incoming call on the called subscriber's terminal.

27. The duty of network operators, service providers and equipment and software suppliers to ensure the privacy of the users should not be interpreted as forbidding member states to regulate, in one way or another, the use of cryptographic algorithms in order to be able to get clear and comprehensible texts in cases where telecommunications have been intercepted on the orders of the authorites, according to the rules set forth in Principles 2.4 and 4.2, and taking into account the guarantees in question.

Furthermore, the drafters of the recommendation accepted that steps taken in accordance with this principle should allow for the possibility of legitimate interference with the content of communications in accordance with Principles 2.3 and 2.4.

28. It will be noted that the protection envisaged in this recommendation is not limited solely to subscribers to telecommunication services or telephone services. It extends to "users" as well as "correspondents". A reference to users is justified by reason of the fact that privacy issues arise when non-subscribers, for example those using a private branch exchange at the place of work, also generate service data. As regards correspondents, it will be seen that the provision of detailed bills to subscribers may have privacy implications for the parties called by the subscribers. For these reasons, it was felt necessary to include both users and correspondents within the scheme of protection.

The recommendation does not explicitly refer to "co-users", because these would in most cases be unknown to network operators and service providers, who would deal exclusively with the subscriber.

29. There is a key role for the classic concept of the right to private life within the framework of the scheme of protection envisaged in this recommendation. Reference in particular should be made to the issue of interception of communications which is discussed in Principles 2.3 and 2.4 and which is inspired by the case-law of the European Court of Human Rights in the context of Article 8 of the European Convention on Human Rights. For the purposes of this recommendation, it is important to note that the right to private life is not the only value stressed in Article 8 of the European Convention on Human Rights. The protection enshrined in that provision also extends to guaranteeing the secrecy of correspondence. For the European Court of Human Rights, this guarantee must apply both to telephone conversations as well as to mail. The desire of the Court to make the European Convention on Human Rights technologically relevant should therefore be seen as allowing the complete range of telecommunication services permitting communication or correspondence between subscribers or users to be included within the protection laid down in Article 8 of the European Convention on Human Rights.

30. The approach followed in this recommendation is therefore underpinned by two sets of interlinked fundamental norms: firstly, those laid down in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and secondly, the provisions of Article 8 of the European Convention on Human Rights.

31. Principles 2.3 and 2.4 are devoted to ensuring the inviolability of communications. Principle 2.3 stresses the illegality of any interference by network operators with the content of a communication, unless this is authorised by the subscriber, or for legitimate reasons. By way of illustration, the network operator may be authorised to read telegrams over the

telephone to the subscriber or other persons authorised by him, or for technical reasons it may be necessary for the network operator to look at the message so as to allow it to be stored or transmitted to the subscriber. This may be the case with electronic mail boxes.

32. Although the communication of data to third parties forms the subject of Chapter 4, the drafters of the recommendation thought it useful to specify in Principle 2.3 that the data relating to the content of messages, collected in accordance with this principle, should not be communicated to third parties, subject to Principle 4.2.

33. Principle 2.4, like Principle 4.2, sets out strict provisions modelled on Article 9 of the Data Protection Convention and designed to ensure a legal basis for interference by public authorities with the content of communications including interference for surveillance purposes, to merely identify the called party. The European Court of Human Rights, as noted earlier, has ruled on a number of occasions (for example, the Klass and others case, the Malone case, the Kruslin and the Huvig cases) that practices such as telephone tapping violate the right to private life and secrecy of correspondence guaranteed in Article 8, paragraph 1, of the European Convention on Human Rights. Any derogation from this fundamental right must be in conformity with its paragraph 2 of Article 8.

34. The references in Principle 2.4 to the use of listening or tapping devices or other means of surveillance should be understood as applying to the use of devices or other means which by their very nature are designed to interfere with telecommunications, whether by way of interception or otherwise.

35. As regards the expression "when this is provided for by law", the drafters of the recommendation understood this to refer to domestic law.

36. Principle 2.5 aims at protecting the data of a subscriber whose communication has been the subject of interference by public authorities. It is clear that in the case of interference on the conditions set out in Principle 2.4, the rights of access and rectification of the data subject have been temporarily suspended (Article 9 of the Data Protection Convention). However, domestic law should regulate the possibility for the data subject to exercise his or her rights once this suspension is no longer effective. The law should also indicate the conditions under which the public authorities concerned may refuse access (for example, danger of prejudicing investigations, existence of overriding public interests, or overriding interests of a third party) as well as conditions under which the data may be stored, or must be destroyed.

37. Principle 2.5 does not guarantee the right of access of a subscriber to his data collected by means of interference by public authorities; it merely requires that domestic law regulate the exercise of such right and the conditions on which the information to the person concerned can be refused. For example, domestic law may provide for a system whereby a person can appeal to an independent judicial authority against allegedly unlawful interception of his or her telecommunication, and when the interception is not found to be unlawful, be notified of that conclusion without any further information on whether the interception has or has not been made. Such procedure, if it provides a framework of safeguards against any arbitrary or unreasonable use of statutory powers in respect of an individual in the position of an applicant, has been recognised by the European Commission of Human Rights, when it held "that states may legitimately fear that the efficacy of a system might be jeopardised by the provision of

information to complainants and that the absence of such information cannot in itself warrant the conclusion that the interference was not necessary (that is, in a democratic society)" (Application No. 21482/93, Christie v. UK).

38. Moreover, to emphasise the inviolability of communications, even when interference does take place, Principle 2.5 specifies that data collected in this way should be communicated only to the body designated in the authorisation for such interference. Communication of this information by the designated body is not governed by this recommendation.

39. Reference should also be made to the principles laid down in the recommendation of the Committee of Ministers regulating the use of personal data in the police sector (Recommendation No. R (87) 15).

40. Unfortunately the telephone is an easy means of causing distress to subscribers. Hoax calls to the emergency services, abusive calls or just the simple communication of malicious messages to subscribers at random are an unfortunate hazard of the telephone service. To combat these types of abuses, Principle 2.6 provides for the possibility for technical means to be employed so as to trace the identity of the culprit, in particular where the calls are repeated and not one isolated incident. Subscribers who are tormented by such calls may request that a particular in-coming call be monitored with a view to identifying the calling party. In some countries it may be necessary to seek an order from a judicial authority before call-tracing may be carried out. Domestic law should determine the degree of proof which must exist in regard to a particular caller before calls may be monitored. At the very least, there should exist a reasonable suspicion against the caller.

41. With regard to the expression "domestic law", the drafters of the recommendation referred to paragraph 39 of the explanatory report of the Data Protection Convention: "39. The 'measures within its domestic law' can take different forms, depending on the legal and constitutional system of the state concerned: apart from laws they may be regulations, administrative guidelines, etc. Such binding measures may usefully be reinforced by measures of voluntary regulation in the field of data processing, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the convention."

42. It will be seen later (Principle 7.17) that one of the reasons which may justify the network operator in overriding a subscriber's decision to suppress his number and to prevent it from being displayed on the terminal of the called party is to identify the source of abusive or malicious calls.

III. Collection and processing of data

44. The risks which developments in this sector present for privacy were alluded to in the preamble. It should, however, be recalled that protection of privacy is not solely limited to shielding the individual from intrusion by public powers into his personal sphere. It rather is to be seen more in terms of the determination of the conditions under which the individual's personal information can be lawfully collected and processed by third parties in both the public and private sectors. This new view of privacy protection in terms of informational self-determination and which is translated throughout the recommendation by the need to ensure that the subscriber or user is accorded rights at the various processing stages, explains the

reference in Principle 3.1 to the Data Protection Convention. This international treaty provides the basis of the principle of informational self-determination as it is to be applied in national law. The provisions of this recommendation are intended to give greater precision to that basis in the sector under examination.

In particular, the Data Protection Convention's principle of "purpose specification" (Article 5.b) is given greater precision so as to adapt it to the realities of information collection and storage by network operators and service providers. The recommendation identifies a number of lawful purposes for which personal data may be collected and processed:

- connecting a user to the network: before becoming a subscriber, the individual will need to give the network operator certain data;

- making available a particular telecommunication service: this may require the publication of certain data in a directory;

- billing and verification: this will require the collection and processing of data concerning the number called, the number from which the call was made, the length of the call, and so on. The network operator may also need to process data on subscribers who do not settle their bills;

- ensuring the optimal technical operation of the network and services: for example it may be necessary to store data so as to determine the volume of calls at particular periods, or to correct errors;

- the development of the network or the services may require collection and processing of data.

44. As with data subjects in general, subscribers to telecommunication services, including telephone services, should not be cut out of the information circuit. The data collected and processed by third parties concern them. Accordingly, they have a right to know as far as possible which data will be collected and processed, on which legal basis this will be done, the purposes for which they will be collected, the uses which may be made of them and the periods over which they will be stored. To make this principle effective, it is necessary to introduce a degree of transparency into the informational activities of network operators and service providers. This is the objective of Principle 3.2. which is, in fact, a reflection of the need to collect and process personal data fairly and lawfully (Article 5.a of the Data Protection Convention).

45. In accordance with the provisions of Principle 3.2, network operators and service providers should inform their subscribers of:

i. The categories of personal data which are being collected and processed

For example subscribers should be told that the network operator stores data provided by the subscriber at the time of application to be connected to the network. In addition, a subscriber should be informed that the network operator collects and processes certain data at the time that the communication is being made, in other words the called number and the length of time spent on the telephone call. Moreover, the subscriber should be informed that the data which

appear in the directory (which may not be the same as the data provided at the time of applying for the telecommunication or telephone service) are also stored by the network operator.

ii. The legal bases of collection

The subscriber should be informed by virtue of which legal text his or her data are collected.

iii. The principal purposes for which the personal data are collected and processed

To fulfil this requirement the network operator or service provider should inform the subscriber that the service data are only collected and processed so that a bill may be sent to the subscriber. As regards the personal data furnished by the subscriber at the time of applying for a telephone service, the network operator should clearly indicate that these data are simply stored to allow the subscriber to be provided with the service and to be connected to the network, and possibly to ensure that he or she does not seek to apply again under an assumed name so as to conceal the fact that he or she has avoided payment of bills.

iv. The use made of the data

Here the subscribers should be clearly informed of the fact that any departure from the lawful purposes indicated under ii. requires authorisation on their part. For example, where basic data is to be used for marketing purposes, then the safeguards listed in Principles 7.7 to 7.11 should be invoked.

The "appropriate manner" in which this information may be provided ranges from references, in the initial contract between the subscriber and the network operator, to the possibility of including the information in the telephone directory. Moreover, network operators or service providers could remind subscribers of the factors listed in Principle 3.2 at the time of dispatch of the bill to the subscriber.

46. The information referred to in this principle should also extend to bringing to the attention of subscribers the rights referred to in Principle 5.1 and the ways and means of exercising those rights.

47. For the reasons set out in paragraph 37 above, it is clear that Principle 3.2 does not apply to personal data which have been collected by network operators and service providers in accordance with Principles 2.4 and 2.5.

IV. Communication of data

48. Principles 4.1 to 4.4 of the recommendation set out a number of guidelines which are intended to regulate the circumstances in which personal data, whether content data, service data or basic data may be communicated to third parties.

Principle 4.1 refers to the general rule that no personal data should be communicated without the written consent of the data subject, or when such communication could lead to identification of the called party.

Principle 4.2 lists the conditions which must be fulfilled before personal data may be communicated to public authorities.

Principle 4.3 indicates the various aspects which must be regulated by domestic law for the communication of personal data to public authorities.

Principle 4.4 discusses the situation in regard to the transmission of subscriber lists to third parties for any legal purpose, including for direct marketing purposes and in that respect is linked to Principles 7.7 to 7.11.

Principle 4.5, finally, deals with communication of personal data between network operators and service providers.

49. Data on the contents of communications should, in principle, not be collected by network operators and service providers, except in the exceptional cases described in Principles 2.3 and 2.4.

50. The circumstances in which service data may be communicated to private bodies or individuals are few. It is, however, possible to imagine requests for communication of service data being made by research companies who are engaged in analysing use of the telephone or other telecommunication services in particular localities. Principle 4.1 requires the subscriber to give his or her express and informed consent in writing before his or her service data may be made available to such bodies. In addition, given that service data may reveal the identity of a subscriber's correspondents, it is necessary to ensure that the data to be communicated do not allow their identities to be determined. With this in mind, anonymisation techniques should be used to conceal the identity of subscribers who have been called from the subscriber's terminal.

51. The data subject may revoke his or her consent, but for obvious reasons this withdrawal will not have a retroactive effect.

52. As will be seen in Principle 7.13, service data for billing should be deleted by the network operator following the payment of the telephone bill by the subscriber.

53. The point has frequently been made in the course of this commentary that particular caution is needed when determining the conditions governing use and communication of service data. By their nature, service data are revelatory of human circumstances: for example, they reveal from where the call was made, the time of the communication and the length of the communication as well as the number called. As a consequence, the drafters of the recommendation have sought to place service data within the fundamental principle of correspondence or communication secrecy as laid down in Article 8 of the European Convention on Human Rights, and reflected also in Article 9 of the Data Protection Convention. It is significant that the Court of Human Rights has, by means of its evolutive interpretation of Article 8, ruled that the communication of such data without the knowledge of the subscriber must be in conformity with the strict provisions of paragraph 2 of Article 8. Referring to the judgment of the Court in the Malone case, it was stated that:

"The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8. The records of

metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8." 1

54. It is for this reason that Principle 4.2 takes over the wording of paragraph 2 of Article 9 of the Data Protection Convention. Accordingly, the communication of service data to public authorities without the consent of the subscriber must be:

a. provided for by law as interpreted by the European Court of Human Rights in cases such as the Malone case;

b. constitute a necessary measure, as interpreted by the Court of Human Rights in the Malone case and be in the interest of one of the factors laid down in Principle 4.2.

55. The drafters of the recommendation agreed that Principle 4.2 does not prevent communication of personal data between network operators or service providers and a statutory regulatory authority, when such communication is necessary for the latter to carry out its duties under domestic law.

56. Network operators and service providers could, under the conditions set out in Article 9 of the Data Protection Convention, communicate data to public authorities, but not to public bodies.

57. Moreover, the recommendation requires in Principle 4.3 that domestic law should regulate a number of aspects when personal data are communicated to public authorities: the exercise of the rights of access and rectification, the refusal by the public authorities to supply information to the data subject, and the conservation or destruction of data communicated to public authorities.

58. The references in Principle 4.3 to rights of access and rectification and to the conditions under which competent public authorities shall be entitled to refuse to give information to the data subject shall be understood as permitting rights of access and rectification to be denied when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences.

59. Principle 4.4 allows that subscriber lists, that is lists processed by network operators and service providers of the basic data of all subscribers - regardless of their inclusion in a directory - are communicated to third parties for any (legal) purpose, including not only marketing purposes, but also opinion polls, statistical surveys, marketing studies and so on, if one of a number of conditions has been met. The drafters of the recommendation acknowledged that these conditions might to a certain extent overlap each other, but emphasised that they were alternative and not cumulative.

60. Such subscriber lists are a valuable source of personal data, particularly for marketing purposes. The information listed therein may be used to enrich other data files so as to gain a more precise view of potential consumer populations for particular products or services. The availability of directories on CD-Rom or magnetic media and the technique of downloading

allow marketing firms increased possibilities for targeting their potential clients whether by linking up the data with other data files or simply by retrieving by automated means lists of names which tend to reveal certain characteristics of subscribers, for example their nationality or their age group. The latter possibility is, of course, a practice which carries with it serious risks for private life since it gives rise to the creation of profiles through the interlinkage of different data sets and the exploitation of personal data outside their authorised context. Names and addresses or telephone numbers cannot be considered as data of relative insignificance to private life. The fact that names may give a clue to nationality or ethnic origin, especially if they can be automatically brought together in lists, makes it essential to determine the conditions governing their use by third parties.

61. With these considerations in mind, Principle 4.4 seeks to condition the communication of subscriber data with respect to certain safeguards. Principle 4.4 is inspired by the approach taken in the earlier recommendation of the Committee of Ministers on the protection of personal data used for purposes of direct marketing (Recommendation No. R (85) 20, and Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies). The text of Principle 4.4 recognises that communication of subscriber lists, notably by telematic means or by the physical delivery of magnetic tapes, may be made subject to either:

a. obtaining the express and informed consent in writing of the subscriber; or,

b. informing subscribers at the time of concluding the initial contract with the network operator that they have the right to object to the communication of their subscriber data to third parties for marketing purposes, and for this purpose may have their name placed on a no-publicity list; or,

c. the authorisation of the authority responsible for implementing and applying data protection legislation; or,

d. a corresponding provision in domestic law.

Principle 4.4 offers these varying degrees of safeguards in an alternative, and not cumulative way so as to reflect the situation in the different member states of the Council of Europe.

62. The provisions of Principle 4.5 authorising the communication of service data between network operators and service providers for the purposes laid down therein are a simple recognition of the need at times for technical co-operation between different network operators and service providers so as to allow telephone calls to be made.

V. Rights of access and rectification

63. Principle 5.1 takes over the rights laid down in Article 8 of the Data Protection Convention. To enable rights of access and rectification to be effectively exercised network operators and service providers should ensure that the data which they hold on subscribers can be easily retrieved when access to them is sought. Accordingly, if the information is located on different data files, ways should be found to enable the totality of the data to be brought together.

64. Access to the data held by network operators or service providers will be of primary benefit to those subscribers who do not request a detailed bill to be sent to them. Principle 5.1 will allow them to obtain from the network operator or service provider a list of the calls which they have made in order to check the accuracy of their telephone bills.

65. The recommendation also attaches great importance to the exercise by the subscribers of the rights of access to their personal data and of rectification of these data because network operators and service providers may, under Principles 2.3 and 2.4, have collected content data. The conditions in which access to and/or rectification of personal data may be refused, limited or postponed by network operators or service providers are therefore set out in Principle 5.2 and correspond to the strict provisions under Article 9 of the Data Protection Convention.

66. The drafters of the recommendation agreed, however, that requests for access to personal data would not always have to be satisfied, if satisfaction of such requests would cause network operators or service providers an unreasonable amount of time or manpower.

VI. Security

67. Data security is a cardinal component of a data protection policy. While earlier principles are intended to address the question of individual vulnerability through the collection and processing of personal data in this sector, Principles 6.1 and 6.2 are devoted to systems vulnerability. The principles are modelled on Article 7 of the Data Protection Convention. The onus is on the network operator to take the best possible measures to secure the network against the threat of unauthorised interference with message transmission or unauthorised interference or access to the various categories of data stored. Personnel should be given clear instructions on the importance of respecting data and network security, as well as training on how to achieve this. In addition, they should be instructed on the importance of maintaining the principle of communications secrecy.

68. As regards data security, the following factors should be taken into consideration: access control to prevent unauthorised persons gaining access to computer systems processing personal data; storage media control to prevent unauthorised reading of storage media; memory control to prevent unauthorised memory inputs or any unauthorised manipulation of stored personal data; access control to ensure that named authorised users of a data processing system can access no personal data other than those to which their access right refers; input control so that it will be possible to check and verify at what times and by whom the various categories of personal data have been processed; organisational control to ensure that staff are aware of data security measures and of the need to respect them.

69. As regards interference with, or surveillence of, communications in course of transmission, network operators should ensure the security of telecommunications lines, and the network in general.

70. Subscribers should be informed of the role they can play in implementing a security policy. As noted earlier in regard to mobile telephones, if encryption techniques are available, mobile telephone subscribers should use them. Furthermore, subscribers to facsimile machines should avoid sending sensitive messages via facsimile. Where the messages left on an answering machine can be listened to at a distance, subscribers should ensure the security of

their remote interrogators. The electronic mail box should be protected by access codes or smart cards which are securely managed by the subscriber.

VII. Implementation of principles

a. Directories

71. Principles 7.1 to 7.6 address the safeguards which should accompany the compilation and use of automated directories, produced by network operators and service providers for the accomplishment of their functions, including the off-prints of such directories. Although the principles are primarily concerned with telephone directories, it should be borne in mind that the development in telecommunication services has produced a range of additional directories for subscribers, for example the popularisation of mobile telephone and facsimile machines has given rise to service-specific directories. The recommendation aims in particular at telephone directories since they constitute the largest source of publicly available personal data. It is precisely the ease of consultation of lists of telephone subscribers as well as the availability of such lists in both manual as well as automated form which has led the drafters of the recommendation to envisage a number of safeguards for subscribers.

72. Moreover, the increased tendency to use subscriber data as a basis for commercial and marketing strategies, particularly by network operators themselves, is just one of the reasons which has led the drafters of the recommendation to advocate Principle 7.1, namely the right of the individual subscriber to exclude himself from the directory. There are other reasons why individuals may wish to have ex-directory rights over and above the simple wish to avoid commercial harassment, whether by telephone or by post. The fear of malicious or abusive calls is also a frequent justification for not wishing one's name to appear in the directory, as is a simple desire to preserve anonymity.

73. These considerations have led the drafters of the recommendation to put forward an ideal solution towards which the governments should work - the right of each subscriber to be excluded from the directory on request, without payment of a fee and without having to justify his or her request. This principle is based on the belief that ex-directory facilities are not a service provided by the network operator but a means which should be freely available to individuals to enable them to protect their privacy and maintain their anonymity.

74. If the first sub-paragraph of Principle 7.1 states the desired goal, the subsequent two sub-paragraphs seek to move states which have different rules in this respect towards the same goal by minimising the restrictions on the exercise of the right in question.

75. Firstly, where the subscriber is legally obliged to enter certain details concerning his or her station in the directory, he or she should nevertheless have the possibility of being exempted from having to prove to the satisfaction of the network operator that the publication of his or her name and number would have adverse consequences, for example an exposure to abusive calls or that the nature of his or her professional activity requires preservation of anonymity.

76. Secondly, in those countries where the payment of a fee is demanded of a subscriber who wishes to go ex-directory, the fee should be set at a reasonable level and within the means of any subscriber who wishes to take advantage of this facility. It may be noted at this juncture that network operators sometimes justify the levying of a fee on the basis that the increased

numbers of subscribers taking advantage of ex-directory facilities places an additional burden on the directory enquiries service. It is felt that this justification will lose much of its substance with the move towards electronic directories which will allow the service to operate much more quickly.

77. As noted earlier, the principles contained in this recommendation are not simply limited to ensuring protection for subscribers. The recommendation is also concerned with extending the safeguards to users. A particular problem in regard to subscriber lists concerns the situation of co-users of a principal subscriber's terminal. The principal subscribers may wish to have their names and addresses (and possibly other information) included in the directory. In accordance with Principle 7.2 any subscriber wishing to do so must prove to the satisfaction of the network operator that the co-users of his or her terminal (for example, the adult members of his household, or persons sharing accommodation provided by the subscriber) have given their consent to their inclusion in the directory.

78. How much data may be required of the subscriber for inclusion in the directory? If Article 5.b of the Convention stipulates that personal data collected and stored must not be excessive, bearing in mind the purpose in question, then Principle 7.3 interprets this as meaning, in the context of subscriber data, that the data to be published should be sufficient and necessary for fulfilling the purpose of a directory, namely to allow members of the public to find the telephone number of a named subscriber. For this purpose, and bearing in mind the recommended right for subscribers to have access to ex-directory facilities, the data to be published should be limited to the surname, sometimes including the forename or forenames to avoid confusion over subscribers with similar surnames, and with the possibility of simply including the initials of the forename, the street name, and, in some cases, just the postal code. However, publication of names and full addresses is not excluded if that is in accordance with domestic law and practice. Network operators should be sensitive to the need to respect the wishes of female subscribers not to have their forenames published. Principle 7.3 accepts that any subscriber may express the wish to have further personal details included in the directory, for example, degrees, titles or professional qualifications.

79. The drafters of the recommendation acknowledged that the expression "personal data necessary to identify reasonably" should be interpreted in the light of the existing practices which might vary from one country to another. In some cases, on request, the address of the subscriber might be included in a directory if this would be a reasonable solution to the problem of homonyms.

80. As far as electronic directories are concerned, Principle 7.4 recommends that technical means to prevent abuse, particularly unauthorised remote downloading, be installed, and that the practice of data matching be restricted.

81. The drafters of the recommendation were also aware of the relation between Principle 4.3 and Principle 7.4. However, where Principle 4.3 regulated the communication to public authorities of complete lists of subscribers, care was taken in Principle 7.4 to make it clear that it applied only to a service rendered by network operators and service providers: to supply specific information in reply to precise queries, and only in respect of data appearing in the directory. In domestic law, measures should be taken to avoid abuse of directory inquiry services.

82. Individuals without immediate access to a telephone directory may seek to find the telephone number of their correspondent by contacting the telephone inquiries service. Under Principle 7.5, provided that the number sought is not ex-directory, the inquiries service may release the number. In some countries it may be possible for the directory inquiries services to contact ex-directory subscribers to see if they wish their number to be communicated to an inquirer. This may be the case where the inquirer is insistent. In these sorts of situations the final decision to communicate the number rests with the subscriber and not the service.

83. May the directory inquiries service release more than just the number of a subscriber, for example, the address of the subscriber or any other details which are to be found in the published directory? The directory is a convenient and practical method of locating the address of a person even if the intention is not to telephone. Does the situation differ when the information is sought through the directory inquiries service? The drafters of the recommendation were aware that abuse of the system had to be prevented, for example information must not be given when the inquirer does not know the name of the person sought. However, the directory inquiries service must be allowed to supply information identical to that appearing in the paper or electronic directory (thereby ensuring equal treatment for persons having a videotex or Minitel at their disposal and those using a directory inquiries service).

84. Lastly, Principle 7.6 refers to the provisions in Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies. In order to cater for the problem, this reference would raise for states where telephone directories are not considered as public files, and for states which have entered reservations in respect of Recommendation No. R (91) 10, the reference is restricted to "the relevant principles" in Recommendation No. R (91) 10.

b. Use of data for the purposes of direct marketing

85. Principles 7.7 to 7.11 apply to all forms of direct marketing, including not only commercial marketing, but also political marketing and approaches made by trade unions, charitable organisations, and so on.

86. As set out above, Principle 4.4 of the recommendation seeks to provide guidance on the sort of conditions and safeguards which should govern the communication of subscriber lists to third parties for any legitimate purpose, including direct marketing, opinion polls, statistical surveys and marketing studies. It should be noted that the approach is modelled on the provisions of Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing. Principles 7.7 to 7.11 which deal with the use of such data for direct marketing purposes, borrow from the same recommendation and, in fact, refer to that recommendation. Although Recommendation No. R (85) 20 is specifically stated to apply to telemarketing, it has been felt appropriate to provide further guidance on how to minimise the privacy risks surrounding this commercial practice by means of telecommunications given that it has evolved as a technique since the adoption of the earlier recommendation.

87. As regards the way in which subscriber data may be used by third parties for marketing purposes, marketing firms, direct mail firms, and so on should bear in mind that subscribers have certain rights in regard to the mailing or marketing lists which have been compiled on the

basis of directory information or which have been communicated to them by network operators in accordance with the provisions of Principle 4.4. In the first place, subscribers may at any time on request have their data erased or removed from the marketing lists held by users. Moreover, they have the right to obtain and rectify data concerning them which are contained on direct marketing lists or files. Furthermore, appropriate measures should be taken to enable subscribers to exercise these rights and to identify the controller of the marketing file. Other relevant principles are laid down in Recommendation No. R (85) 20.

88. It goes without saying that subscribers have a right to opt out of inclusion of their data in directories in accordance with the provisions of Recommendation No. R (85) 20. They should also have the right to appear in lists which indicate to the network operator that they do not wish to receive any marketing or promotional material. Principle 4.4 lists a number of other protective safeguards which enable subscribers to prevent their names being included on marketing lists. All these factors should be respected when marketing firms or direct mail companies seek to exploit subscriber data. This issue is important since Recommendation No. R (85) 20 enables any person "to collect personal data for direct marketing purposes from files open to the public and other published material". As noted previously, telephone directories are among the most important of the public files in existence. Nevertheless, the fact that the telephone directory is public does not mean that the data contained in it should not be protected. It is for this reason that Principle 2.2 of Recommendation No. R (85) 20 envisages restrictions being laid down by domestic law aimed at the indiscriminate exploitation of personal data contained in public files for marketing purposes. As regards the telephone directory, the safeguards mentioned above which allow the subscriber to opt out either from the telephone directory, or from the receipt of marketing or promotional material, or from the communication of his data to third parties for marketing purposes, constitute appropriate restrictions in the eyes of the drafters of the recommendation.

89. Reference should also be made to Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies which also lays down certain criteria which should be respected by marketing firms when they seek to exploit personal data contained in public files. Although the text is relevant to the activities of public network operators, it is believed that the recommendation's principles may also be used by private operators so as to determine the conditions under which subscriber lists may be made available to, and exploited by, marketing and mailing companies.

90. Whilst Principles 4.1 and 4.3 address communication of personal data in general, Principle 7.8 requires that for the use of personal data by network operators, service providers or third parties for the purpose of direct marketing, domestic law provides appropriate guarantees and determines the conditions to be fulfilled.

91. As with Recommendation No. R (85) 20, the present recommendation also stresses the utility of self-regulation as a means of ensuring the appropriate legal and social environment for the practice of telemarketing. With this in mind, Principle 7.9 encourages the sector to elaborate its own codes of practice so as to ensure that telemarketing is only carried out in a way which does not annoy or harass subscribers. Principle 7.9 indicates a number of guidelines which should be incorporated into the codes of practice. Rather than inserting in the appendix a principle on the prohibition of advertising material directed at minors, the drafters of the recommendation agreed that the codes of conduct should discourage this practice.

92. Although self-regulation is emphasised, it needs to be borne in mind that the codes of practice or codes of conduct for telemarketing should be drawn up in accordance with domestic law, for example, data protection legislation. The codes, if they are to be effective and binding on the telemarketing industry, should be approved by a superior authority - for example the authority entrusted with the implementation of data protection legislation. These references to data protection legislation should not be interpreted as excluding the possibility for consumer legislation to tackle the problems raised by telemarketing and allowing self-regulation to take place within the framework of laws designed for the protection of consumers.

93. Principle 7.10 obliges companies engaged in telemarketing - and it is recognised that this includes marketing by telephone, facsimile, electronic mail or other telecommunication means which allow messages to be transmitted - to respect the wishes of subscribers who do not want to receive advertising material. Accordingly, those subscribers whose names appear on a "no publicity" list, or who are ex-directory, or who in some other way have asked not to receive marketing material, should not be contacted by telemarketing companies. To respect their wishes, Principle 7.10 encourages the service providers to keep a list of those subscribers.

94. The above considerations in regard to telemarketing apply to network operators and service providers as well as any other body which may market by means of telecommunications.

95. Specific consideration is given to the issues raised by automatic calling devices, including the facsimile. These robotic dialling devices allow for the random dialling of pre-recorded marketing messages. They feed on lists of numbers which are dialled over and over again until the subscriber replies. Principle 7.11 states quite clearly that the use of such devices for transmitting pre-recorded messages of a marketing nature may be directed only at those subscribers who have given their consent to this sort of service ("opting in"). These devices may also be used for purposes other than marketing. For example, they may be used to inform subscribers of information concerning sports results or share movements. In these circumstances, the subscriber will usually have paid for, and thus consented to, for the service.

96. The text is silent on the issue of using pre-recorded messages so as to alert subscribers living in a particular neighbourhood of a local emergency. They may also be used to inform the population at large of national emergencies. This practice is acceptable. It may also be the case that a subscriber may be contacted by the network operator so as to warn him in a pre-recorded message that his telephone will shortly be cut off for non-payment of his telephone bill. It is felt that the subscriber should consent to this type of pre-recorded message at the time of signing his initial contract with the network operator. Otherwise, the transmission of the message may be both intrusive and the cause of embarrassment to the subscriber. It may also be the case that network operators will send pre-recorded messages to subscribers that a telegram has arrived for them and they are requested to pick it up at a particular post office. This practice may also be deemed to be acceptable but subscribers should be informed at the time of signing their contract with the network operator that messages such as these may be sent in a pre-recorded manner to them.

97. Bearing in mind these considerations, it is felt that the number of circumstances in which pre-recorded messages should be sent should be as limited as possible.

c. Detailed billing

98. Itemised bills to subscribers listing the calls which they have made over a certain period of time, the numbers called, the time spent on calls, and so on, present enormous consumer advantages. It enables subscribers to determine the accuracy of the bill which has been sent to them by the network operator and to contest the bill if they believe

it to be incorrectly calculated. It is thus not surprising that in some countries consumers have campaigned very strongly for the introduction of itemised bills.

99. Nevertheless, urgent data protection problems are raised by the provision of itemised bills to subscribers, as well as by the retention by the network operator of the service data on which the bill is based. Firstly, the provision of an itemised bill to a subscriber enables him or her to examine the telephone use of other people living in the household. In particular, it allows the principal subscriber to identify the correspondents of the co-users. Secondly, the fact that the service data are stored by the network operator exposes them to the risk that they will be used for purposes other than billing. This risk must be diminished by ensuring that the bill is not retained for a long period by the network operator. Possible solutions to these problems have been advanced in Principles 7.12 and 7.13.

100. Confronted with this possible conflict of interests, the drafters of the recommendation endeavoured to find an acceptable compromise. Principle 7.12 makes the provision of an itemised bill to a subscriber optional. In addition, where the subscriber's telephone is placed at the disposal of other users - for example the adult members of the family - consideration should be given to avoid obstructing their freedom to use the telephone as a result of the making available to the subscriber an itemised bill setting out their telephone transactions. Although one argument may be that co-users use the subscriber's telephone at their own risk, the subscriber should at least inform them of the fact that he or she will receive detailed bills on a regular basis which will reveal information concerning their use of the telephone. They will then be in a position to act accordingly.

101. Regarding the listings of the numbers called from the subscriber's telephone, as noted earlier, the privacy of the correspondents becomes an issue. For this reason, network operators might provide detailed bills in a manner which makes it difficult or impossible to identify the subscriber of the called number. Some countries have already developed practices in this regard. With these practices in mind, consideration could be given to deleting the last few figures of the telephone number called.

102. Although anonymisation of numbers called should be encouraged, the complete bill may, in fact, be stored by the network operator. If this is the case, then subscribers should be informed of this practice in accordance with the information requirement referred to earlier in Principle 3.2. Unless legal provisions would require those data to be kept longer, data needed for billing must be deleted following payment of the bill by the subscriber, bearing in mind the fact that the data may need to be stored for a reasonable period in the event of the subscriber issuing legal proceedings to contest the accuracy of the amount owed. In any event, the data must be deleted at the close of the proceedings or the settlement of the case or when the deadline for legal storage has expired (Principle 7.13).

d. Private Branch Exchange Systems (PBX systems)

103. The recommendation is not solely limited to protecting the users of private and public telecommunication networks which have an official status - for example because they are public monopolies or because they have been granted concessions to compete with these monopolies. Within companies, private branch exchanges are normally set up so that the personnel within organisations may communicate by telephone. Private branch exchanges are also found in establishments such as hotels where there is demand for telephone facilities. The use of such private branch exchanges gives rise to the storage of service data. For example, the owners of the network are obliged to store data so that the user may be billed for the time spent on the telephone call. The calculation of the bill would obviously involve the identification of the office or hotel room from which the call was made, the number called and the duration of the call.

The drafters of the recommendation agreed that companies, hotels, hospitals, restaurants and so on, who made available to their employees or clients an internal telephone service, would come under the definition of "service provider" and, therefore, fall within the scope of the recommendation.

104. Principle 7.14 of the recommendation seeks to introduce transparency into the collection and processing of service data by operators of private branch exchanges. As a general rule, it should be brought to the attention of the user of a telephone (or another telecommunication facility such as a facsimile or electronic mail) that the use of the telephone gives rise to the storage of service data. While Principle 7.15 refers to Recommendation No. R (89) 2 on the protection of personal data used for employment purposes, Principle 7.14 merely recommends that outside the employment context "appropriate means" should be found so as to inform users of data storage accompanying their use of the telephone. These "appropriate means" could take the form of hoteliers placing stickers on the telephone terminals in the hotel rooms or information leaflets in the hotel rooms beside the telephone. The service data should be erased immediately after the bill has been paid by the user.

105. The drafters of the recommendation recognised that it is not always the user who pays the bill. It may be forwarded to another party - for example an employer - for payment. In any case, Principle 7.12 applies also to PBX systems: in principle, the bill provided by the operator of a private branch exchange should be presented and transmitted to the third party in a way which respects the privacy of the caller. The bill should only refer to the amount owed without referring to the nature of the calls made.

106. Principle 7.15 devotes special consideration to the introduction and use of telephone logging systems at the place of work and is based on Recommendation No. R (89) 2. This recommendation is inspired by the need to ensure that the collection and storage of service data are carried out fairly and lawfully and that the data are not used for purposes such as monitoring the time spent by employees on the office telephone with a view to drawing conclusions on matters such as their productivity or attitude to work.

e. Calling-line identification

107. The digitalisation of networks has made possible this new service feature in voice telephony. With the aid of a display unit on a subscriber's terminal, it is now possible to identify the source of incoming calls, that is the identity of the calling party. Several countries in Europe have already introduced this service feature. Other countries envisage allowing ISDN subscribers the possibility of identifying the telephone numbers of callers still linked to the analogue network.

108. This new service feature brings with it many advantages for subscribers. Firstly, it allows them to be in control when the telephone rings. With the incoming number displayed even before the communication takes place, the subscriber is in a position to decide whether or not to speak to the calling party. Secondly, the new service feature is a useful tool to combat abusive or malicious calls since those responsible for them will no longer be able to conceal their identity (provided of course that they are telephoning from a terminal connected to the ISDN network). Thirdly, the display of the incoming number on the called party's terminal presents obvious advantages for emergency services such as police, ambulance and fire brigade. In brief, it allows such services greater possibilities for identifying the location of distressed callers who may not always be in a position to communicate clearly their location and predicament.

109. The perceived advantages indicated in the preceding paragraph need to be evaluated in the light of a number of possible privacy problems which have been identified by the data protection community. Firstly, the service feature may possibly undermine the anonymity which is guaranteed by ex-directory facilities. Secondly, calling-line identification constitutes an obstacle to the freedom of communication of individuals contacting help-line services, such as Alcoholics Anonymous, advice centres or the Samaritans. Individuals are encouraged to contact these sorts of agencies on the basis that their anonymity will be respected. Subscribers will obviously be discouraged from telephoning help-lines if they know that their telephone number will be revealed. A similar problem exists in regard to confidential lines set up for the purposes of police enquiries. Thirdly, the release of a telephone number to a commercial or marketing agency as a result of a telephone enquiry regarding a particular product or service may give rise to unwanted calls of a commercial or marketing nature.

110. It is against the background of these problems that Principle 7.16 requires subscribers to be informed that calling-line identification is being made available. Moreover, the drafters of the recommendation agreed on the usefulness of the calling party being able to suppress the display of his or her telephone number on the called party's terminal. This could be achieved by, for example, the incorporation into telephone terminals of a simple technical device such as a push button facility which when pressed would allow the caller to maintain anonymity. The recommendation does not require that the calling party should be able to have the display of his or her number cancelled on a permanent basis (so preserving the advantages of ex-directory facilities), or on a call-by-call basis as a possible, but not mandatory alternative to the permanent suppression of the display.

111. Whilst it was generally accepted that calling parties who had a legitimate interest in keeping their anonymity should have the possibility of preventing disclosure of their telephone

numbers, the drafters of the recommendation agreed that the costs of providing such a facility to called parties as well would, for the time being, outweigh their interests.

112. The drafters of the recommendation agreed also that in view of the ongoing discussions in some states, it would be premature to require that no additional costs should be incurred by a calling party for suppression of calling-line identification.

113. In certain circumstances, it may be necessary to override the calling party's decision to press the button and maintain his anonymity. For example, emergency services (the police, the fire brigade, and so on) should always be able to have access to the calling party's number. Furthermore, a subscriber harassed by malicious or abusive calls or emergency services troubled by hoax calls, may instruct the network operator to cancel the instructions given by the calling party to the network. This decision is not to be taken lightly and it is for this reason that Principle 7.17 provides that domestic law should determine the conditions and safeguards which must exist before this may take place.

f. Call forwarding

114. Call forwarding allows a user to reroute his incoming calls to the terminal of a third party. This service is not dependent on the digitalisation of the network, since it has always been available in the analogue system. Principles 7.18 and 7.19 of the recommendation seek to lay down some guidelines which will ensure the comfort of third parties to whom incoming calls are transferred by called subscribers.

115. Firstly, the third party should be informed before the subscriber takes the decision to forward incoming calls to the third party's terminal. Secondly, in case of disagreement, the third party should be able to cancel the forwarding.

Because, on the one hand, the recommendation is, in principle, not addressed to subscribers and, on the other hand, the responsibility of subscribers themselves should be developed, the drafters of the recommendation did not wish to include a requirement that subscribers should inform a third party subscriber of their intention to have incoming calls forwarded to the latter's terminal.

The recommendation provides, however, that in case of dispute a possibility should be offered to cancel call forwarding (Principle 7.18).

116. It will be noted that the recommendation does not address the situation in which calling parties are not made aware of the fact that a call is being re-routed to the terminal of a third party. While there may be justification in allowing the calling party to be informed of this fact, the drafters of the recommendation have also noted the security risks which this presents. It is thought undesirable to inform calling parties of the fact that the called party is not at home.

117. Principle 7.19 discusses the situation in which a tapping or a listening device has been placed on a subscriber's telephone in accordance with the provisions of Principle 2.4, and the subscriber has transferred his or her in-coming calls to a third party. There is a possible technical risk that the third party and his or her circle of correspondents will be caught up in the net. It is for this reason that Principle 7.19 advocates that, insofar as this is technically

possible, only the incoming calls of the suspect should be subject to surveillance measures to the exclusion of incoming calls for the third party.

118. As was the case with Principle 2.4 (see paragraph 34 above), the reference in Principle 7.19 to surveillance measures should be understood as applying to the use of devices or other means which by their very nature are designed to interfere with telecommunications, whether by way of interception or otherwise.

g. Mobile telephones

119. The speed with which the mobile telephone service has been taken up by subscribers, sometimes inspired by fashion trends, has tended to overlook the serious problems to which their use gives rise. The recommendation has identified two issues which should be addressed:

i. the vulnerability of mobile telephones as a means of communication;

ii. their capacity to give rise to the storage of service data which may interfere with the private life of the user.

120. In addressing the issue of vulnerability, the recommendation notes that the use of the mobile telephone service lacks a secure means of maintaining the confidentiality of communications. Interception of conversations is easier. This presents a problem for the use of car telephones by government ministers or businessmen. With this in mind, Principle 7.20 proposes that network operators should inform their subscribers of the vulnerability of message transmission by means of mobile telephones. Although Principle 7.20 does not expect the network operator to provide an encryption service so as to increase the security of message transmission, it is nevertheless felt that ways should be found to offer subscribers the possibility of availing themselves of methods of encryption.

121. As was the case with Principle 2.2 (see paragraph 27 above), the duty under Principle 7.20 for network operators and service providers to find a means of offering encryption possibilities, or equivalent safeguards to subscribers to mobile telephone networks should not be interpreted as forbidding member states to regulate, in one way or another, the use of cryptographic algorithms in order to reproduce clear and comprehensible text in cases where the contents of telecommunications have been intercepted upon order of the authorities, according to the applicable rules, and taking into account the guarantees in question.

The means for offering encryption possibilities or equivalent safeguards should be such as to allow for the possibility of legitimate interference with the content of communications in accordance with Principles 2.3 and 2.4.

122. As regards the storage of service data, account should be taken of the fact that the mobile telephone network will shortly be digitalised, thus allowing subscribers to transmit via their car telephones facsimile messages, vocal messages, images and data. As with the digitalisation of the generalised networks, the amount of service data stored by the operators of the mobile telephone network will considerably increase. As far as the generalised networks are concerned, it becomes increasingly important to define precisely the purposes for which the service data can legitimately be held by the network operator offering mobile telephone facilities. Storage should be restricted to the following purposes: connecting the subscriber to

the network and processing the service data to enable the bill to be sent to the subscriber. While it is admitted that the location of the user will have to be recorded when he or she logs into the system so as to determine the zone in which he or she is to be found, as well as location at the time of making calls, Principle 7.21 seeks to ensure that these data are not used for determining the movements of the user or the identity of his or her correspondents. These risks have led the drafters of the recommendation to suggest that the data required for drawing up bills should be based on wide geographical areas rather than precise details of the exact location of the user when he or she changes zone or makes a call, which is all that is necessary for the application of the relevant scale of charges. It is felt that the system of tariffs could reflect this proposal.

Footnotes

1. Hereinafter referred to as "the Data Protection Convention".

2. New technologies - a challenge to privacy protection?, Strasbourg, Council of Europe, 1989, ISBN 92-871-1616-4.