EUROPEAN UNION
THE COUNCIL

Brussels, 10 November 1998

10951/1/98

REV 1
LIMITE

ENFOPOL 98

TRANSLATION SUPPLIED BY THE PRESIDENCY

NOTE

from : Austrian Presidency

to : Police Cooperation Working Party

No. prev. doc.: OJ C 329, 4.11.1996, p.1 ; 10102/98 ENFOPOL 87 ; 10951/98 ENFOPOL 98

Subject : **Interception of telecommunications**
- Draft Council Resolution on new technologies

Preliminary remark

The delegations will find attached the revised draft version of the Council Resolution on Interception of Telecommunications in Relation to New Technologies.

This version was compiled at two IUR Expert Meetings (20 - 22 October 1998 in Vienna and 27 - 28 October in Madrid).

It was agreed to make a reference in the actual text of the (new) Council Resolution that the requirements of 17 January 1995 are applicable both to existing and new technologies, these requirements needing supplementary explanatory detail as a result of progress in telecommunications technology.

In Part 1 (Requirements) and Part 2 (Glossary) the provisions of the requirements 1995 are listed, explained and supplemented. Part 3 contains additional requirements and explanations. With regard to other technical areas which are indirectly related to the actual interception requirements (e.g. cryptography, call-associated and subscriber-related data), additional technical descriptions will be required. After completion, these might be published together with the Requirements 1995 and the above mentioned explanations and supplementary detail in a technical handbook.

D R A F T

COUNCIL RESOLUTION

of .....

on the Lawful Interception of Telecommunications in relation to New Technologies.

THE COUNCIL OF THE EUROPEAN UNION

(P R E A M B L E)

HAS ADOPTED THIS RESOLUTION:

1. The Council considers that the requirements of law enforcement agencies in regard to network operators and service providers for the purposes of lawful interception of telecommunications, as described in the Council Resolution of 17 January 1995 (96/ 329/01) are applicable both to existing and new technologies, for example satellite communications and the Internet.

2. The Council notes that, as a result of progress in telecommunications technology, the requirements have to be explained.

3. The Council further considers that progress in telecommunications technology has created a need for supplementary explanatory detail, including security measures and subscriber-related data in regard to network operators and service providers.

4. The Council considers that the aforementioned explanation and supplementary detail as annexed should be taken into account in the implementation of measures for lawful interception of telecommunications and requests Member States to call upon the Ministers responsible for telecommunications to support this view and to co-operate with the Ministers responsible for Justice and Home Affairs with the aim of implementing the supplementary detail and definitions in relation to network operators and service providers.

Part I : Explanation of Requirements

(The normal text correspondence to the requirements.
The bold text are explanations)

Note : The Internet requires specific explanations.

1. Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call.

1.1 Law enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system.

1.2 Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications services or terminal equipment, including calls that traverse more than one network operator/service provider before completing.

1.3 Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

1.4 Law enforcement agencies require access to call associated data such as:

1.4.1 Signalling of access ready status.

1.4.2 Called party number for outgoing connections even if there is no successful connection established.
Note : Called party number includes any identifier of the called party.

1.4.3 Calling party number for incoming connections even if there is no successful connection established.
Note : Calling party number includes any identifier of the calling party.

1.4.4 All signals emitted by the target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer.

1.4.5 Beginning, end and duration of the connection.

1.4.6 Actual destination and intermediate directory numbers if call has been diverted.

1.5 Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

1.6 Law enforcement agencies require data on the specific services used by the interception subject and the technical parameters for those types of communication.

2. Law enforcement agencies require a real-time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.
Notes : In this conntext and in relation to call associated data, data is required within a few seconds.

3. Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/ service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries.

3.1 Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

3.2 Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format. This format will be agreed upon on an individual country basis.

3.3 If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

3.4 Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

<u>Note</u> : Switched connections includes all types of switched connections including circuit-switched and packet-switched connections. IP connections are not excluded.

3.5 Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable security requirements.

Note : Further security requirements are detailed in the attached paper.

4. Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

5. Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Note : Further security requirements are detailed in the attached paper.

5.1 Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

5.2 Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

5.3 According to national regulations, network operators/service providers could be obliged to maintain an adequately protected record of activations of interceptions.

6. Based on a lawful enquiry and before implementation of the interception, law enforcement agencies require:
   (1) the interception subject's identity, service number or other distinctive identifier,
   (2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and
   (3) information on the technical parameters of the transmission to the law enforcement monitoring facility.

   Note : Further subscriber-related data requirements are detailed in the attached paper.

7. During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

   Note : Further explanation concerning number portability is detailed in the attached paper.

8. Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements.

   Note : For international systems the maximum number of simultaneous interceptions needs to be derived from combining national requirements.

9. Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by country and by the type of target service to be intercepted.

10. For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

Part II : Explanations of the Definitions in the Glossary of the Council Resolution of 17 January 1995 (OJ 96/C 329/019)

(The normal text correspondence to the requirements.The bold text are explanations)

ACCESS

The technical capability to interface with a communications facility, such as a communications line or switch, so that a law enforcement agency can acquire and monitor communications and call associated data carried on the facility.

Note : In this document access refers to interception access for the law enforcement agencies.

CALL

Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.

Note : In this document a call includes any connection irrespective of the technology of the network, e.g. packet-switched networks.

CALL ASSOCIATED DATA

Signalling information passing between a target service and the network or another user. Includes signalling information used to establish the call and to control its progress (e.g. call hold, call handover). Call associated data also includes information about the call that is available to the network operator/service provider (e.g. duration of connection)

INTERCEPTION

As used here, the statutory based action of providing access and delivery of a subject's telecommunication and call associated data to law enforcement agencies.

INTERCEPTION INTERFACE

The physical location within the network operators/service providers telecommunications facilities where access to the intercepted communications or call associated data is provided. The interception interface is not necessarily a single, fixed point.

Note: In some telecommunications technologies the interception interface may be a virtual interface within the network.

INTERCEPTION ORDER

An order placed on a network operator/service provider for assisting a law enforcement agency with a lawful authorised telecommunications interception.

INTERCEPTION SUBJECT

Person or persons identified in the lawful authorisation and whose incoming and outgoing communications are to be intercepted and monitored.

LAW ENFORCEMENT AGENCY

A service authorised by law to carry out telecommunications interceptions.

LAW ENFORCEMENT MONITORING FACILITY

A law enforcement facility designated as the transmission destination for the intercepted communications and call associated data for a particular interception subject. The site where monitoring/recording equipment is located.

LAWFUL AUTHORISATION

Permission granted to a law enforcement agency under certain conditions to intercept specified telecommunications. Typically this refers to an order or warrant issued by a legally authorised body.

NETWORK OPERATOR/SERVICE PROVIDER

N e t w o r k o p e r a t o r = the operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means; and
S e r v i c e p r o v i d e r = the natural or legal person providing (a) public telecommunications service(s) whose provision consists wholly or partly in the transmission and routing of signals on a telecommunication.

QUALITY OF SERVICE

The quality specification of a communications channel, system, virtual channel, computer-communications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

RELIABILITY

The probability that a system or service will perform in a satisfactory manner for a given period of time when used under specified operating conditions.

ROAMING

The ability of subscriber of mobile telecommunications services to place, maintain, and receive calls when they are located outside their designated home serving are.

TARGET SERVICE

A service associated with an interception subject and usually specified in a lawful authorisation for interception.

TELECOMMUNICATION

Any transfer of signs, signals, writing, images sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.

Part III. Additional Requirements / Explanations

a) for INTERNET

Individual Telecommuncations over the Internet is subject to the IUR 95.
In this context number or other electronic identifier means e.g. fixed and dynamic IP adresses (the electronic address assigned to a participant in the Internet), account numbers and e-mail addresses.
Call associated data are not separate from the call content (esp. for requirements 1, 1.4. to 1.4.6, 2, and 3.1).

b) SECURITY

The growing amount of cross-border co-operation in the field of telecommunications interception requires a parallel level of security in the respectiv countries.