EUROPEAN UNION
THE COUNCIL

Brussels, 4 November 1994 (08.11)
(OR. d)

10571/94

RESTREINT

ENFOPOL 150

OUTCOME OF PROCEEDINGS

from: Steering Group II

to : K.4 Committee

No. prev. doc.: 9898/94 ENFOPOL 132

Subject: Draft Council Decision on the lawful interception of telecommunications

DRAFT COUNCIL DECISION

OF

on the lawful interception of telecommunications

The Council,

Having regard to the Treaty establishing the European Union [in particular Articles K.1(9) and K.2(2) thereof;]

Having regard to the secrecy of communications protected by the constitutions and laws of the Member States, the European Convention on Human Rights and the principles of data protection;

Having regard to the possibilities provided for in the laws of the Member States for restricting the secrecy of communications and, under certain circumstances, intercepting telecommunications;

Whereas the legally authorized interception of telecommunications is an important tool for the protection of national interest, in particular national security and the investigation of serious crime;

Whereas interception may only be effected insofar as the necessary technical provisions have been made;

Whereas in accordance with a decision by the TREVI Ministers in December 1991 a study should be made of the effects of legal, technical and market developments within the telecommunications sector on the different interception possibilities and of what action should be taken to counter the problems that have become apparent,

has adopted this Decision:

1. The Council notes that the requirements for conducting the legally authorized interception of telecommunications, annexed hereto ("the Requirements"), equally constitute an important summary of the needs of the competent authorities as users for the technical implementation of legally authorized interception in modern telecommunications systems.

2. The Council considers that the aforementioned Requirements should be taken into account when the legally authorized interception of telecommunications is defined and implemented, and calls on the Ministers responsible for telecommunications to support this view and to cooperate with the Ministers responsible for Justice and Home Affairs, so that the Requirements may in fact be implemented as part of national telecommunications policy.

For the Council of the European Union
The President

REQUIREMENTS

This section presents the Requirements of law enforcement agencies relating to the lawful interception of telecommunications. These requirements are subject to national law and should be interpreted in accordance with applicable national policies.

Terms are defined in the attached glossary.

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 or are processed by 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

1.4.3. Calling party number for incoming connections even if there is no successful connection established

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, fulltime 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.

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.

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

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.

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 inquiry 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.

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.

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.

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.

GLOSSARY

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.
Call	Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.
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 telecommunications and call associated data to law enforcement agencies.
Interception Interface	The physical location within the network operator's/service provider's telecommunications facilities where access to the intercepted communications or call associated data is provided. The interception interface is not necessarily a single, fixed point.
Interception Order	An order placed on a network operator/service provider for assisting a law enforcement agency with a lawfully authorized telecommunications interception.

Interception Subject	Person or persons identified in the lawful authorization and whose incoming and outgoing communications are to be intercepted and monitored.
Law Enforcement Agency	A service authorized 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 of a particular interception subject. The site where monitoring/recording equipment is located.
Lawful Authorization	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 authorized body.
Network Operator/Service Provider	– "network operator" = 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; – "service provider" = 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 telecommunications network.
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 subscribers of mobile telecommunications services to place, maintain, and receive calls when they are located outside their designated home serving area.
Target Service	A service associated with an interception subject and usually specified in a lawful authorization for interception.
Telecommunications	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.