COUNCIL OF THE EUROPEAN UNION

Brussels, 20 June 2001 (OR. en)

9194/01

LIMITE

ENFOPOL 55
ECO 143

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject :	Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services

COUNCIL RESOLUTION

of

on law enforcement operational needs
with respect to public telecommunication networks and services

THE COUNCIL OF THE EUROPEAN UNION,

Recalling the objectives of the Treaty on European Union;

Bearing in mind the Council Resolution of 17 January 1995 on the lawful interception of telecommunications; [1]

Reaffirming the need, when implementing telecommunications interception measures, to observe the right of individuals to respect for their privacy;

Considering that criminals, like anyone else, use telecommunications in pursuit of their objectives and that they take advantage of opportunities offered by telecommunications systems both to avoid detection and to commit offences;

[1] OJ C 329, 4.11.1996, p. 1.

Convinced that lawful access to these telecommunications is vital in the investigation of serious crime and the prosecution of offenders;

Aware of the impact on lawful interception of new and emerging technologies in telecommunications;

Bearing in mind that the aim of the Resolution of 17 January 1995 was to provide a platform for discussion with Telecommunications Providers on Law Enforcement Agencies' operational needs rather than imposing legal obligations on them;

Taking into account the ongoing work of Law Enforcement Agencies to cooperate with the telecommunications industry in discussions of operational needs and means of meeting them;

Aware of the fact that the Resolution of 17 January 1995 described the operational needs of the Law Enforcement Agencies, but that the development of new technologies has made it necessary for some further explanation;

Noting the requirements of Member States to continue and maintain lawful interception capabilities;

Considering that the Annex to this Resolution constitutes an important summary and explanation of the operational needs of law enforcement agencies in taking account of new and emerging technologies,

HEREBY ADOPTS THIS RESOLUTION:

The Council calls upon Member States to ensure that, in the development and implementation – in cooperation with communication service providers – of any measures which may have a bearing on the carrying out of legally authorised forms of interception of telecommunications, the law enforcement operational needs, as described in the Annex, are duly taken into account.

ANNEX

Law Enforcement Operational Needs

Contents

General

Subject to national legislation, all kinds of telecommunications may be subject to interception and/or data searches in relation to enquiries. This document relates to the operational needs of Law Enforcement Agencies (LEAs) with respect to public telecommunication networks and services. It does not recommend technical specifications or solutions but is a set of guidelines for technical discussions, which will be needed for implementation.

Applicable Services

This document applies to all telecommunications services, circuit and packet switched, fixed and mobile networks and services.

For fixed networks this includes, for example, PSTN and ISDN (Integrated Services Digital Network). For packet switched networks and services this includes, for example, GPRS, UMTS (Universal Mobile Telecommunications System), xDSL, TETRA (Trans European Trunk RAdio standard), Email/message services and other Internet telecommunications services. For PLMN this includes, for example, GSM (Global System for Mobile communications), CDMA, IS41, AMPS, GPRS, UMTS, TETRA. It also applies to S-PCS (Satellite Personal Communication Systems).

Law Enforcement Operational Needs

General Observations

The International User Requirements (IURs), see OJ C 329, 4.11.1996, p. 2, were written at a time when telecommunications were predominantly circuit switched. Although this may have influenced the terminology used throughout the IUR, law enforcement's needs are technology neutral. The IUR expresses law enforcement's general operational needs regardless of technology even if some of the terms used, e.g. "call", appear to limit their scope to specific technologies. More detailed clarification of this and other terms is provided throughout this document.

Throughout the document, each IUR item is presented first, followed by explanations/clarifications where applicable. The items are presented in functional rather than numerical order.

Access to Telecommunications

> [IUR 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.

"Call" in this context means the entire telecommunications transmitted, or caused to be transmitted, to and from the entity associated with the number or other identifier specified in the legal authorisation. "Number" or "Identifier" is the means by which telecommunications facilities determine specific communications. Identifiers may refer to a physical or logical entity (e.g. user addresses, equipment identities, user name/passwords, port identities, mail addresses, etc.) and may differ according to the type of telecommunications system.

Typical, but not exclusive, examples for some specific services are: For PLMN IMSI, MS-ISDN, IMEI; for PSTN/ISDN directory numbers, port identification, personal and vanity numbers; for Internet (access) services IP addresses, account number, logon ID/password, PIN number and E-mail address.

Law enforcement needs the transmitted and received components of intercepted telecommunications to be delivered such that those components can be handled separately. (For example, this applies in telephony-like networks to ordinary calls between A and B party, conference calls, etc.).

Contemporaneous telecommunications should be handled in such a way that it is possible clearly to distinguish between them. (Some examples of telephony-like networks are enquiry calls, simultaneous forward calls, etc).

Law enforcement needs any telecommunications associated with the identifier of the subject of interception.

"Call Associated Data" should be understood as being "Communications Related Data" throughout the document. (See explanation under IUR 1.4 for more detail).

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

Law enforcement needs access to telecommunications even when the subject of an interception is a temporary user of a network or telecommunications facility. (Some illustrative examples are: in PLMN roaming; in telephony-like systems UPT and calling cards; in Internet services remote access via other service providers, etc.).

> [IUR 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.

As stated above, "Call" should be understood as "Telecommunications". Law enforcement needs any telecommunications associated with the identifier of the subject of interception. (Examples for telephony-like systems are diversion of calls or direct communication to a voicemail box).

Access to Communications Related Data

> [IUR 1.4] Law enforcement agencies require access to call associated data such as:

The needs explained in 1.4 apply to all telecommunications services. However, the information resulting from the interception will depend on the telecommunication service (e.g. conference calls, call-forwarding, mobile calls, network calls, call-back services, etc.). For packet switched services this information could already be part of the packets.

NB: similar data to those referred to in 1.4 are needed not only when such data are received as a result of interception but also where they have been retained by providers in accordance with the requirements of their national legislation.

[IUR 1.4.1] signalling of access ready status;

1.4.1 expresses the need for an indication that the user facility is being logged on, or connected, to the telecommunications service.

[IUR 1.4.2] Called party number for outgoing connections even if there is no successful connection established;

[IUR 1.4.3] Calling party number for incoming connections even if there is no successful connection established;

1.4.2 and 1.4.3 express the need to be aware of all the numbers or identifiers related to attempted telecommunications involving the interception subject. This applies whether or not the telecommunications to or from the interception subject are successful.

[IUR 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;

1.4.4 expresses the need for access to all signals emitted by the interception subject and particularly applies to signals that activate or facilitate telecommunications facilities (e.g. re-routing). They may reside within the telecommunication but should not necessarily be considered as part of the content of that telecommunication service.

[IUR1.4.5] Beginning, end and duration of the connection;

1.4.5 expresses the need for the most accurate time stamps the telecommunication system can provide on telecommunications and on telecommunications–related signals. (In most cases there will be no need to calculate the duration).

[IUR 1.4.6] actual destination and intermediate directory number if call has been diverted.

1.4.6 expresses the need for the provision of numbers or identifiers involved in the telecommunication when re-routing is invoked by users.

> [IUR 1.5] Law enforcement agencies require information on the most accurate geographical location known to the network for a mobile subscriber.

1.5 expresses the need for location information which may be geographical, physical or logical. Even fixed networks facilitate mobility by means of services such as personal numbering/UPT, dial-in networks for ISPs (Internet Service Providers), re-routing, etc.

The type of information provided will depend on the network, but should be as accurate as possible.

It should also be presented in a form that is easily interpreted.

> [IUR 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.

1.6 expresses the need for information on the services used in the intercepted telecommunication. This information assists the correct interpretation of the communication content. Some illustrative examples are: bearer services in ISDN; the bearer and tele-services in GSM, etc.

Conditions for Access

> [IUR 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 authorisation.

1.3 is self-explanatory, but it should be noted that fulfilling the need in detail will depend on individual national jurisdictions.

> [IUR 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.

2 expresses the need for telecommunications to be provided to the intercepting agency without undue delay. This will depend on the typical performance of the technology used and any special conditions imposed (e.g. for security, see also IUR 3.5).

Provision of a real time and full time monitoring capability might require resilience. The means used to achieve this capability will depend on the intercepted technology (e.g. circuit or packet switched) and national jurisdictions.

Delivery of Interception Product

> [IUR 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 is self-explanatory.

> [IUR 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.

3.1 expresses the need for correlation. This may be intrinsic in some technologies where communications-related data are delivered together with telecommunications content. However, where this is not the case, a reliable method for correlation should be used. (For example, time references are not acceptable because they may be ambiguous e.g. Standard Time, Summer Time, and where simultaneous communications can be in progress).

> [IUR 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.

3.2 is self-explanatory.

[IUR 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.

3.4 is self-explanatory, but it should be noted that the term "service providers" applies to all telecommunications providers. "Switched connections" include both circuit and packet services.

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

3.5 expresses the need for transmission of intercepted telecommunications to be performed in such a way that the confidentiality and integrity of the product are maintained. The product may be used as evidence for both defence and prosecution purposes; the confidentiality needs to be maintained both to meet privacy considerations and for investigative reasons.

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

5.2 is self-explanatory and applies to all telecommunications providers.

Security of the Interception Facility

> [IUR 4] Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorised 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.

4 is self-explanatory, but it should be noted that telecommunications services or networks must be capable of performing interception without indicating this to other services or networks.

> [IUR 5] Law enforcement agencies require the interception to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the interception.

5 is self-explanatory, but it should be noted that security considerations cover issues such as unauthorised access to facilities, site and personnel security.

> [IUR 5.3] According to national regulations, network operator/service providers could be obliged to maintain an adequately protected record of activations of interceptions.

5.3 is self-explanatory, but it should be noted that the same level of security applies to records of activation as to the interception facilities. The term "activation" also covers cessation and extensions.

> [IUR 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.

5.1 is self-explanatory, but it should be noted that it applies to all telecommunications providers.

Access to Information on the Subject of Interception

[IUR 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.

6(1) and (2) express the need for information which will support LEAs' requests for interception. Typical information required about the subject of interception includes: a technical identifier; the full name of the person (or company) subscribing to the service; the residential address of the subscriber (or registered business address of a company); the postal address to which accounts are sent; credit card details sufficient to identify the account; the directory name if applicable (note that this may differ from the subscriber's name); the directory address if applicable (note that this may differ from the residential or postal address).

6(3) does not directly relate to the subject of interception but is necessary for the general support of interception.

Other Assistance

> [IUR 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.

7 is self-explanatory.

> [IUR 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.

9 expresses the need for administrative facilities and technical designs which enable providers to implement interception efficiently.

Access to Multiple and Simultaneous Interceptions

> [IUR 8] Law enforcement agencies require network operators/service providers to make provision 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 that confidentiality of the investigations. The maximum number of simultaneous interception for a given subscriber population will be in accordance with national requirements.

8 is self-explanatory and applies to all telecommunications providers.

Reliability of the Interception Facility

> [IUR 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 operator/service provider.

10 is self-explanatory (please also refer to IUR 2).

Encrypted Services

[IUR 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.

3.3 is self-explanatory.

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.
Authenticity	Establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.
Authorised person(s)	A person authorised to perform duties related to lawful interception.
Availability	The property that a communications system or service is useable on a timely basis in the required manner.
Call	Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. Note: generally, the technology neutral term is "telecommunications".
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 include information about the call that is available to the network operator/service provider (e.g. duration of connection). Note: the generally applicable technology neutral term is "communications related data".

Data	The representation of information in a manner suitable for communications, interpretation, storage or processing.
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 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.
Integrity	The property that data or information has not been modified or altered in an unauthorised manner.
IUR	International User Requirement – the common term for the International Requirements for Interception (Version 1.0) and the Council Resolution of 17 January 1995 on the lawful interception of telecommunications (published in the Official Journal of the European Communities C 329, 4.11.1996, p. 1).

Law Enforcement Agency (LEA)	A service authorised by law to carry out telecommunications interceptions. Note : This definition refers to LEAs' function only in terms of this document
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 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	"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) the provision of which 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 service area.
Target Service	A service associated with an interception subject and usually specified in a lawful authorisation 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, photo-electronic or photo-optical system.