

Brussels, 2 June 1995

JHA  
8A.9

4118/2/95

REV 2  
LIMITE

ENFOPOL 1

**N O T E**

---

from : the Presidency

to : the Working Party on Police Cooperation (Interception)

---

No. prev. doc.: 4118/1/95 ENFOPOL 1 REV 1

---

Subject: **Legal interception on telecommunications systems provided outside national boundaries**  
- Report of Expert Sub-Group (Paris, 5 May 1995)

---

Delegations will please find herewith the report of the Expert Sub-Group on the above subject.

**REPORT OF THE EXPERT SUB-GROUP**  
**LEGAL INTERCEPTION ON TELECOMMUNICATIONS SYSTEMS**  
**PROVIDED OUTSIDE NATIONAL BOUNDARIES**

**1. Summary**

Planning is well advanced on the next generation of mobile personal telecommunications systems. Unlike the existing terrestrial systems (e.g. GSM) the next generation will operate through satellites which in many cases will provide the service from outside national boundaries. These new systems provide unique opportunities to those involved in serious and organized crime and those who constitute threats to national security or the economic well-being of the state. Similarly they also pose unique problems for legal interception. Moreover, many of these planned systems will be owned and operated by consortia of major international companies. This paper sets out the rationale behind the systems, a timetable for their introduction and the difficulty of conventional legal interception. It then discusses opportunities for interception and this is followed by our recommendations. It is worth noting that preliminary contacts with the consortia during our fact finding revealed reaction varying from an extreme willingness to co-operate to an almost total refusal to even contemplate the issue.

Our recommendations, in short, stress the extreme urgency for Government and/or regulatory bodies to make clear to the new consortia what their obligations will be. Governments will also need to establish new regimes of international co-operation to permit the required interception facility to operate.

**2. Description of new systems**

To a considerable degree many of the proposed systems will operate in a similar manner. Many will incorporate existing GSM technology and will be able to use either GSM or the new system depending on location or choice by the mobile user. The proposed systems will use a varying number of low or medium earth orbiting satellites in different configurations. These satellites communicate, in most cases, with ground stations located in various parts of the world. In one case, there will be communication between the satellites. The ground station can act directly or indirectly as interconnection points <sup>(1)</sup> for a number of surrounding countries - that is to say there will not be a interconnection point in every country.

**3. Chronology of new systems**

The first systems tests are planned in 1995 with public service available in 1998. Several such systems may be in operation by the turn of the century.

---

<sup>(1)</sup> the point of entry into the terrestrial telecommunications system.

#### **4. Specific threats to interception posed by new systems**

- 4.1** Conventional methods of legal interception on the fixed and mobile telecommunications networks are carried out on the national infrastructure. However, it will be clear from the foregoing that conventional methods of legal interception will not be possible in countries that do not host an interconnection point. This means that the operators of these new systems may well fall outside normal jurisdiction for legal interception. It is possible that interconnection points may be located in uncooperative countries. The problem is further complicated by the fact that a target, although operating within a particular national boundary, may be registered in another country.
- 4.2** Other methods of interception, such as monitoring the up and down links, will be difficult because many of the links will be encrypted and carried on narrow beam antennas. In many cases the mobile units will operate on low power towards the satellites and with narrow beamwidths from the satellite. There is practically no possibility of monitoring the up and down links from the mobile units except at extremely close range (hundreds of metres).
- 4.3** It is worth recalling, as an outcome of the Bonn Seminar on Legal Interception, that as well as the content of any particular communication it is also required to produce as soon as possible some call-related data such as the number calling, the number called, any subsequent numbers called, times and durations of the communication and the location of the target. All these features are of vital importance to law enforcement.
- 4.4** Given that subscriber data will be more widely held on these systems, there will need to be extra provision and mechanisms to obtain names, addresses and used subscriber numbers.

#### **5. Possible solutions to interception**

The existing mechanisms for mutual legal assistance in criminal investigation do not fit the needs of the next century. The problems caused by these new systems will require a dynamic and effective mechanism to be instituted. The subject is dealt with in two parts - what is operationally and technically possible and what may be possible through political and regulatory means.

##### **5.1 Operational considerations**

- 5.1.1** In many respects these systems will resemble the architecture used for GSM. This means that because of administration and charging requirements, information on each subscriber must be held permanently (usually at the point at which he registered for service) and temporarily (usually at the point at which the subscriber is operating). It will be possible, if implemented at the design stage, for any particular

subscriber to be "flagged" when an intercept is required. A subscriber is marked for access or denial to particular services depending on his type of subscription. A certain amount of information about any subscriber is therefore verified before he is able to initiate a service. The inclusion of an intercept flag would trigger the appropriate mechanism for interception. The subsequent treatment of the call content and call-related data is discussed in the next section.

- 5.1.2** It is important to note that all these systems are in an advanced stage of design. If facilities are to be built in for legal interception, it is absolutely vital to identify them now. The GSM experience should illustrate the problems where the facilities had to be introduced after the system had been implemented.

## **5.2 Political and regulatory implications**

- 5.2.1** There are a number of issues here and we need to assume firstly that some marking system can be provided. In discussing the political and regulatory implications, we take as an example the extreme case of a subscriber who is a citizen of country A, registered for service in country B, operating temporarily in country C and using a telecommunications system where the interconnection point is located in country D and wishes to make a call to country E. He is the subject of an interception warrant for some serious misdemeanour in country F (see annex A).
- 5.2.2** The first issue is whose legal regulations are applicable and, as a consequence, where is the warrant or legal order to be issued and where to be served ? The country (A) of which he is a citizen is not directly involved either in the misdemeanour or in the carriage of the communication. The country (B) in which he is registered for service, and will pay his bills, is not involved in the misdemeanour or in the carriage of the communication but will provide the authorization data onto which the interception flag can be attached. The country (C) in which he is operating will probably be quite unaware of his presence, is not involved in the misdemeanour and need not be involved in the authorization to operator the carriage of the communications. The country (D) in which the interconnection point is located is not involved in the misdemeanour but is involved in the carriage of the communication and is able to provide the intercept as indicated by the presence of the flag on the subscribers data. The country (E) to which the call is routed is not involved in any of the foregoing but may have certain operating limitations with the provider of the service.
- 5.2.3** The next issue is to agree on the method to handle the content and call-related data across national boundaries. This will require prior agreement on the location of the used interconnection point, on the routing of the material to the handover point, the handover protocols and factors concerning its retention, confidentiality and integrity.

- 5.2.4 The final question is one of costs. The provision of intercept facilities is relatively inexpensive only if incorporated at the design stage. Then there is the cost of operating an intercept system, the carriage of the material and the subsequent processing. It is important that this is structured in such a way as to cause an imperceptible penalty on any particular operator so as not to affect their commercial integrity. This includes, of course, the knowledge that interception is possible.

## 6. CONCLUSION

- 6.1 These new telecommunications systems share characteristics with existing mobile systems, e.g.

- the individual subscriber is mobile ;
- the range of the system is not confined to one state ;
- the subscriber may choose between different competing systems.

However, they differ in one particular aspect in that the systems do not necessarily have an establishment in a specific state.

- 6.2 This means that the state may be powerless to enforce an order against the network operator because the network operator does not have a domicile in this state.
- 6.3 For the enforcement of an intercept order it is essential to have a point of contact situated within the legal order of the state which issued this order.
- 6.4 This is clearly a matter which will develop rapidly into a global problem. It would seem that the solution will require global co-operation of an unprecedented nature.

## 7. RECOMMENDATIONS

- 7.1 It is recommended that the "Requirements of Legal Interception" document be conveyed to the planners, operators and service providers of the new systems as soon as possible to act as a basis for discussion with national authorities.
- 7.2 Ministers should ensure that interception is still possible with these new systems in accordance with the international requirements.

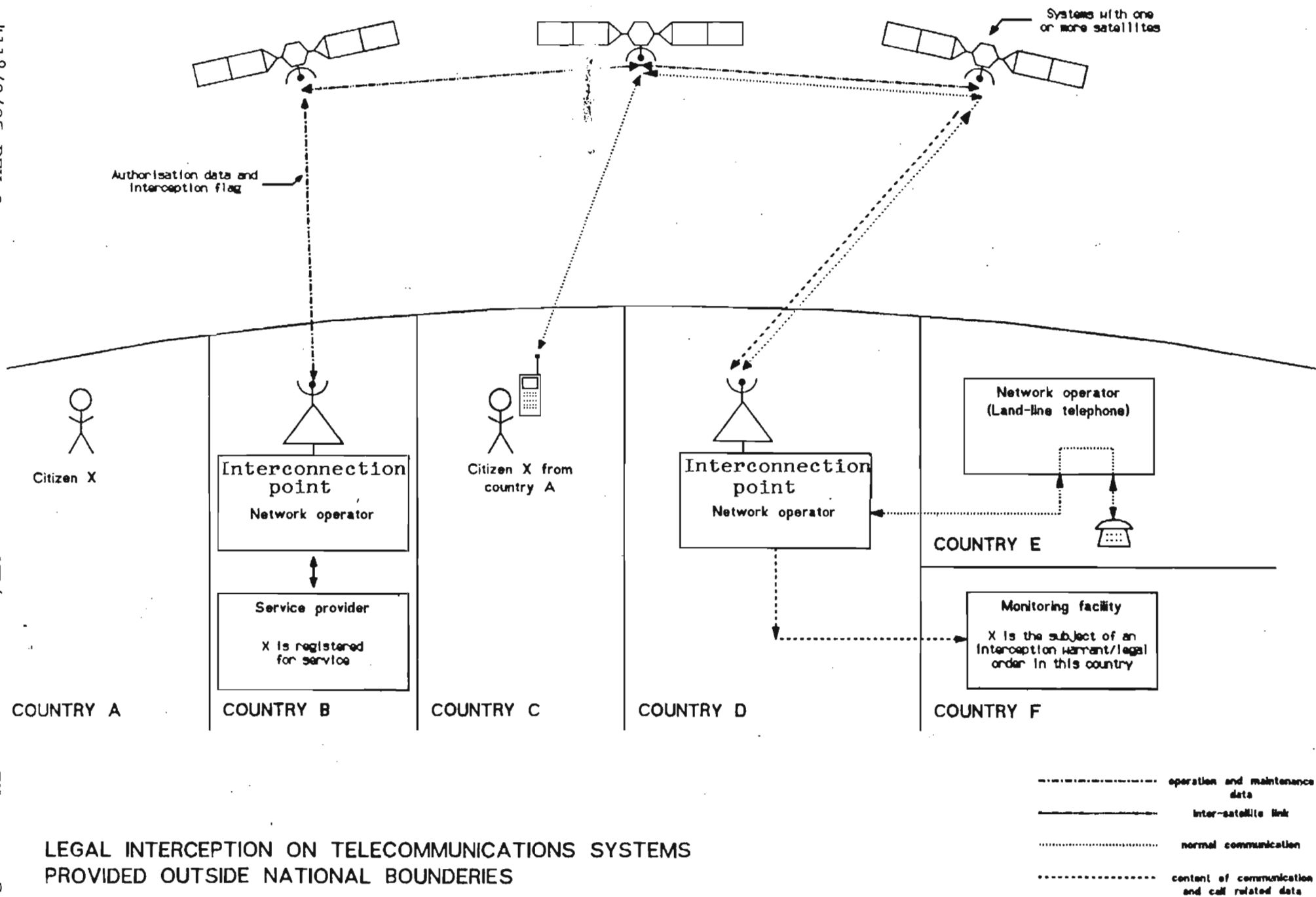
- 7.3** Ministers are asked to ensure that the existing national legislation is reviewed and to develop means of international co-operation for the legal interception of telecommunications.
- 7.4** Ministers are invited to ensure that legal and technical provisions are in place to obtain subscriber-related data such as names, addresses and used subscriber numbers.
- 7.5** Ministers are invited to ensure that an equitable cost regime is developed for international legal interception.
-

4118/2/95 REV 2

WF/an

EN

- 7 -



LEGAL INTERCEPTION ON TELECOMMUNICATIONS SYSTEMS  
PROVIDED OUTSIDE NATIONAL BOUNDARIES