***Statewatch* analysis no 11**

Surveillance of communications: data retention to be “compulsory” for 12-24 months

Draft Framework Decision to make data retention and access for surveillance by law enforcement agencies "compulsory" leaked to *Statewatch*

Contents

Statewatch's analysis of the draft Framework Decision shows that there are "grave gaps in civil liberties protection":

- there are no grounds for refusing to execute a request on human rights grounds
- there are no limits as to what data can be exchanged where member states allow for the retention of data on all crimes, not just the 32 listed
- there is no reference to supervisory authorities on data protection
- there is no reference to the individual's right to correct, delete, block data nor compensation for misuse or for related judicial review
- no reference to controls on the copying of data
- no rules for checking on the admissibility of data searches

Introduction

Tony Bunyan, Statewatch editor, comments:

> *“EU governments claimed that changes to the 1997 EC Directive on privacy in telecommunications to allow for data retention and access by the law enforcement agencies would not be binding on Members States - each national parliament would have to decide. Now we know that all along they were intending to make it binding, “compulsory”, across Europe.*
>
> *The right to privacy in our communications - e-mails, phone-calls, faxes and mobile phones - was a hard-won right which has now been taken away. Under the guise of fighting "terrorism" everyone's communications are to be placed under surveillance.*
>
> *Gone too under the draft Framework Decision are basic rights of data protection, proper rules of procedure, scrutiny by supervisory bodies and judical review”*

Even as the European Parliament was discussing and voting on fundamental changes to the 1997 EC Directive on privacy in telecommunications the Belgian government was drafting (and circulating for comment) a binding Framework Decision on the retention of traffic data and access for the law enforcement agencies - which has been leaked to *Statewatch.*

Under the guise of tackling "terrorism" the EU's Justice and Home Affairs Minister decided on

20 September 2001 that the law enforcement agencies needed to have access to all traffic data (phone-calls, mobile calls, e-mails, faxes and internet usage) for the purpose of criminal investigations in general.

What stood in the way was the 1997 EC Directive on privacy in telecommunications. This was the follow-up to the hard-won 1995 EC Directive on data protection, now law across the EU. The 1997 EC Directive said that the only purpose for which traffic data could be retained was for billing (ie: for the benefit of customers) and then it had to be erased. Law enforcement agencies could get access to the traffic data with a judicial order for a specific person/group.

The "deal" agreed in May between the Council (the 15 governments) and the two largest parties in the European Parliament (PPE, conservative and PSE, Socialist groups) means that there are two crucial amendments: i) the obligation to erase data has been deleted and ii) EU member states are allowed to pass laws requiring communications providers to keep traffic data for a so-called “limited period”.

In June the incoming Danish Presidency of the Council of the European Union (the 15 EU governments) submitted "Draft Council conclusions" on this topic, which contain four Recommendations, to the EU's Multidisciplinary Group on Organised Crime (MDG). The Draft Conclusions say that:

> *“**within the very near future, binding rules should be established** on the approximation of Member States' rule on the obligation of telecommunications service providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for a criminal investigation” (emphasis added)*

One of the arguments used to legitimise the move during the discussions in the European Parliament was that the change to the 1997 Directive simply enabled governments to adopt laws for data retention if national parliaments agreed. The document leaked to *Statewatch* shows that EU governments always intended to introduce an EC law to bind all member states to adopt data retention.

The draft Framework Decision says that data should be retained for 12 to 24 months in order for law enforcement agencies to have access to it. In theory the agencies will still need a judicial order to trawl back through the records of a targeted person(s) - though this legal nicety has never stopped the internal security agencies getting access in many countries.

The traffic data of the whole population of the EU (and the countries joining) is to be held on record. It is a move from targeted surveillance to potentially universal surveillance.

Draft Framework Decision on data retention and access for the law enformcent agencies

Overall analysis

1. The scope is very broad as it would apply to all data in relation to land and mobile telephones and Internet connections.

2. The key provisions are Article 3(1), the obligation of service providers, and Artilce 3(4), governing access by law enforcement authorities to that data for at least the usual list of "Euro-crimes".

3. Articles 3(1) and 3(2) vague as to what exactly will be collected on top of the mandatory list in 3(1) but falling short of content, which is prohibited under this Framework Decision, by Article 3(2). Perhaps this is to cover data on where the mobile phone is located, or collection of data

from a computer or phone other than the content of the conversation? The data collection obligation in Article 3(1) is not limited to traffic data and that 3(1) uses the non-exhaustive wording, "in particular".

4. In Article 3(4) there is a reference to data which is retained during the application of the article then a reference to "traffic data2. Are these two different things and if so, what the first category consists of?

5. There are grave gaps in civil liberties protection even compared to Schengen, the Cyber-crime convention or other recent EU measures like the arrest warrant, despite the references to harmonising procedural guarantees in the preamble. The gaps are:
a. there is no ground for possible refusal to execute a request from another Member State on human rights grounds (ie the arrest warrant, proposals on confiscation and freezing, Article 15 of the Cyber-crime convention)

b. there are no grounds to refuse as regards differences in the scope and timing of data retained under different Member States (although this is vaguely hinted at by Article 7(4) - logically why should the executing authority be allowed to request such data unless it would be able to refuse the request on those grounds). Put another way, if Member State A only gives law enforcement authorities access for the usual list of 'Euro-crimes' and Member State B gives them access for investigating any alleged crime at all (eg: under the UK's Anti-Terrorism, Crime and Security Act 2001 which cover all crimes), can the authorities of MS B contact the authorities of MS A and insist that the latter obtain the traffic data which the service providers have held? Is MS A required or permitted to refuse access? This data could then end up with Europol or various national agencies if it is released; it could even end up back with the law enforcement authorities of MS A - indeed they would gain access to it simply through the process of transmitting it to MS B (this is more likely since there are no controls on copying the information - see below). If the authorities in MS A are unethical they could even ask MS B's authorities to send such a request just so they could escape the constraints in their national law.

c. the term "at least" concerning the 32 offences listed plus the Cybercrime convention suggests that if a member state allows for access to data covering all crimes then this is allowed.

d. there is no reference to the involvement of supervisory authorities on data protection (cf SIS rules)

e. in fact there are no grounds to refuse execution of requests on any grounds, even if it might jeopardise an ongoing investigation;

f. there is no reference to individual rights to access, correction, deletion, blocking of data or compensation for misuse, or for related judicial review to this end (cf the SIS rules), either against the authorities or the service providers/TTPs (also Article 15 of the Cyber-crime convention requires judicial or other review of decisions and sets out a principle of proportionality)

g. there is no reference to controls on the collection or the copying of the data (see SIS rules)

h. there are no rules on a date to review the keeping of data or the destruction of data by the law enforcement authorities (as distinct from the service providers or TTPs, who are subject to limits in 3(1))

i. there are no rules re checking on the admissibility of searches (cf SIS rules)

j. Article 4(1) does not limit access to those authorities who need the data for a specific investigation (3.4 does not expressly do this either)

6. There is one difference in the list of 'Euro-offences' in that there is a reference to the Cyber-crime convention rather than just 'cybercrime'. But this just makes more explicit the underlying problem with the use of such a list on the grounds that the substantive criminal law has been sufficiently harmonised. For the cybercrime convention gives Member States a number of

options to refuse fully or partly to criminalise a number of the acts listed within it, even on matters of such great public concern as child pornography.

7. The 'Eurolist' of offences arguably performs a different function here than in other measures. In all other measures the list abolishes double criminality requirements, whereas here it is not at all clear whether a double crminality requirement could still apply in the absence of the Eurolist.

Article by articles analysis of the draft Framework Decision on data retention

While the European Parliament was still discussing the changes to the 1997 EC Directive on privacy in the telecommunications sector the Belgian government was working on a draft Framework Decision - a measure binding on all EU member states - on the same issue. Indeed one of the argument officials used to legitimate the changes to the 1997 Directive was that it was not binding, it simply allowed member states to introduce data retention if their governments and parliaments agreed.

This "voluntarist" approach was never seriously considered. Since January 1995, when the EU governments adopted the FBI's "Requirements" (to be placed on service and network providers), it has been clear that for the surveillance of telecommunications to work data retention would have to be mandatory for EU member states (and the applicant states). Surveillance requires, at one level, the "real-time" interception of a series of communications. For example, a phone conversation between two people in countries A & B which is immediately followed by the person in country A ringing a person in country C and the person in country B ringing someone in country D. Equally, the same model would apply to the surveillance of e-mail data which would break down if countries B and D did not have the same laws on data retention and access to the data by law enforcement agencies (police, immigration, customs, prosecution service and internal security agencies).

Framework Decision: from non-binding to binding

In June the incoming Danish Presidency of the Council of the European Union (the 15 EU governments) submitted "Draft Council conclusions" on this topic, which contain four Recommendations, to the EU's Multidisciplinary Group on Organised Crime (MDG). The Draft Conclusions say that:

> *"within the very near future, binding rules should be established on the approximation of Member States' rule on the obligation of telecommunications service providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for* ***a criminal investigation****" (emphasis added)*

The four Recommendations proposed are very general: i) "to ensure that law enforcement agencies are able to react immediately and effectively to the new challenges"; ii) to ensure the agencies "receive further training"; iii) to ensure that decisions on interception and access to data is taken quickly, "especially in the case of mobile telecommunications, where the communicating parties can move freely from country to country without warning"; iv) to find solutions to the "increased use of encryption".

The work programme of the Danish Presidency says it: "intends to submit a proposal for a Council Resolution on investigation methods in relation to modern information technology, including the storage of telecommunications data" (3.7.02). In their effect Council Resolutions and Council Conclusions are the same, they are both non-binding and intergovernmental (that is, outside EC Treaties).

While Recommendations, Resolutions and Conclusions are not binding Framework Decisions are. The Danish Presidency declares its intent to "within the very near future" put forward

"binding rules".

The Recitals

The Draft Framework Decision starts with 16 Recitals followed by 10 Articles. In the Recitals it is argued, as is now common, that there is a need for:

> *"maintaining a balance between the protection of personal data and the need of the law and order authorities to have access to data for criminal purposes" (Recital 3)*

This is a balance which is struck in favour of the "law n' order agencies".

Again in Recital 4 is another familiar argument used to legitimise new measures in the EU. The argument involves, including buzz words like "paedophile" and "racism" to justify intrusive new powers (in the 1990s the words were "organised crime" and "illegal immigrants"). Thus the Recital reads:

> *"Access to traffic data is particularly relevant in the case of criminal investigations into cybercrime, including the production of paedophile and racist material"*

The EU's concept of "cybercrime" is itself high problematic and is by no means limited to "paedophile and racist material".

The argument in the next four Recitals (5-8) is that laws in EU member states generally allow access to communications traffic data where authorised by a court or Minister for a specific investigation. "Many Member States" have also, it says, passed legislation requiring compulsory "a priori retention" but "the content of the legislation varies considerably" - the direction of the argument is obvious, there is a need for harmonisation (which would also have the effect of bringing up to speed member states who were not intending to do this). Thus:

> *"These differences present problems... and are prejudicial to cooperation in criminal matters. A harmonisation is therefore desired both by the authorities responsible for criminal investigations and by the providers of telecommunications services"*

In sum:

> *"The purpose of this present framework decision is to make compulsory and to harmonise the a priori retention of traffic data in order to enable subsequent access to it, if required, by the competent authorities in the context of criminal investigation"*

The overall rationale finishes with the bland statement that although the retention of data "constitutes an interference in the private life of the individual" it "does not violate" international laws on privacy "where it is provided for by law and where it is necessary in a democratic society, for the prosecution of criminal offences" (Recital 9). This argument has many potential dangers not the least of which is, what if a law is adopted which undermines a democratic society?

The Recitals then move on to deal with the details. Apparently:

> *"a minimum period of 12 months and a maximum of 24 months for the a priori retention of traffic data is not dispropionate" (Recital 12)*

Recital 14 says that it "would be disproportionate" if the minimum list of "types of data to be retained" was extended "to the content of messages exchanged or of the information sources consulted under whatever form" (eg: pages visited on internet sites). It remains to be seen whether this version will end up in the adopted text - there will be those in the "law enforcement community" who will argue that there is only limited value in keeping only the traffic data but not

the content.

It appears there are likely to be at least four further Framework Decisions. One will cover a "minimum list of data to be retained" by telecommunications service providers. Second, although the draft Framework Decision says that it will not apply "to data at the time of transmission, that is by monitoring, interception or recording of communications" this is coded language for saying than another Framework Decision is in the pipeline (the "real-time" interception of communications was included in the "Requirements" adopted in January 1995). Third, a certificate for the exchange of data between EU Member States. Fourth, we can expect another to cover access to the content of communications.

The Articles

Article 1 covers "Definitions" the most important of which is on "traffic data", defined here as "all data processed which relate to the routing of a communication by an electronic communications network" which is not very illuminating. But there is a footnote referring to the Council of Europe Cybercrime Convention (Article 1 point d) which says:

> *"Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed part of the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service"*

Article 2 would allow access to "the authorities responsible for criminal investigations and prosecutions" - which is interesting in the light of the UK government's attempt to give access to traffic data to some 1,039 public authorities (see Statewatch News online, June 2002).

Article 3.1 says that there will be an "obligation" on a telecommunications service provider or a "trusted third party" (not defined) to retain "for a period of 12 months minimum and 24 months maximum" the following categories of traffic data:

> *a) Data necessary to follow and identify the source of a communication;*
> *b) Data necessary to identify the destination of a communication;*
> *c) Data necessary to identify the time of a communication;*
> *d) Data necessary to identify the subscriber;*
> *e) Data necessary to identify the communication device*

Article 3.2 says that the "types of data" must be:

> *"limited to what is necessary in a democratic society for criminal investigation and prosecution"*

This begs a major question: what is necessary in a "democratic society" is not static. The boundaries for "what is necessary" have expanded leaps and bounds over the past few years and in particular since 11 September. Indeed it has to be asked are there any boundaries?

Article 3.4 sets out a minimum list of 33 "serious" offences to be included, which is the same as set out in the European arrest warrant. They include: trafficking in human beings, computer-related crime, facilitation of unauthorised entry and residence and motor vehicle crime. This same list of offences appears in a number of recent measures (including the Framework Decisions on the European arrest warrant and the Freezing of assets) and looks like becoming a list of "quasi-federal" offences - many have not been harmonised or even defined.

Article 4 sets out "Procedural rules and data protection", which contains no provision on data protection.

The Article again says that access to traffic data retained will on be allowed for:

> *"judicial authorities or, to the extent that they have autonomous power in criminal*

investigation prosecution, to police authorities" (Article 4.1)

It says further that: "Data to which access has not been asked at the end of the mandatory retention are destroyed" (ie: after 12 or 24 months).

Article 4.2 says nothing in this Article limits national laws which cover: "access to data during their transmission, including tracking, interception and recording of telecommunications".

Articles 5-8 deal with requests and the exchange of traffic data between the "competent authorities" of EU Member States.

Thus Article 6 defines "competent authorities" as follows:

> *"The issuing authority shall be the authority of the issuing State which is competent to issue a decision of access to retained traffic data by virtue of the law of the issuing State" (Art 6.1)*

Under the proposal of the UK government, that was withdrawn for re-consideration after a public outcry, a "competent authority" could be any one of the 1,039 "public authorities" authorised under the Regulation of Investigatory Powers Act 2000 - for which there is no comprehensive oversight in place.

The "executing authority" (ie: the authority agreeing to the request) shall be a "judicial authority of the executing State" (Art 6.2).

Article 7 sets out the procedure for the exchange of data. The "issuing authority" will send a request to the "executing authority" in the form of a "certificate" which will simply cover:

a) the issuing authority;
b) information allowing to identify the provider of telecommunication services which must have retained the traffic data;
c) the criminal conduct under investigation;
d) indications allowing to select the searched data among all retained data"

The "executing authority" is allowed (Article 7.4) to ask for "further information to enable it to decide whether access to retained data would be authorised in a similar national case". However, if the "issuing state" simply states that the "criminal conduct under investigation" is one of the 33 listed crimes there is no apparent reason why further information would be required.

Article 7.5 deals with the special situation of the UK and Ireland who are not yet full members of the Schengen Convention on policing matters. The UK and Ireland may state in a declaration the "central authorities" to be notified "when the provisions on mutual assistance of the Schengen Implementing Convention are put into effect for them". Article 8 "Conditions of execution" appears to allow Member States, like the UK, who want to authorise hundreds of "authorities" to request access, to apply the same rules when answering a request. Implementation of the Framework Decision is set for 31.12.03 (Article 9.1)

Sources: see Statewatch, vol 7 no 1 & 4 & 5; vol 8 nos 5 & 6; vol 10 no 6; vol 11 nos 1 & 2 & 3/4; vol 12 no 1 & 3/4.

Full-text: draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions

THE EUROPEAN COUNCIL

In view of the European Union Treaty, and in particular article 29, article 34, paragraph 2, point b;

In the light of the proposal by .....

In the light of the opinion of the European Parliament,

Considering the following:

1. Offering a high level of protection in an area of liberty, security and justice requires that criminal investigations and prosecutions be carried out in an adequate manner.

2. The use of telecommunications services has grown to the extent that the data relating to this use, and principally those relating to traffic are very useful tools for investigating and prosecuting criminal offences.

3. The conclusions of the Council of 20 September 2001 call for care to be taken to ensure that the forces of law and order are able to investigate criminal acts which involve the use of electronic communications systems and to take measures against the perpetrators of these, while maintaining a balance between the protection of personal data and the need of the law and order authorities to have access to data for criminal investigation purposes.

4. Access to traffic data is particularly relevant in the case of criminal investigations into cybercrime, including the production and diffusion of paedophile or racist material. The plan of action of the Council and the Commission on the best ways to implement the provisions of the Treaty of Amsterdam on the establishment of an area of liberty, security and justice, the conclusions of the European Council at Tampere on 15-16 October 1999, the European Council at Santa Maria del Feira on 19-20 June 2000, the European Commission in its scoreboard and the European Parliament in its resolution of 19 May 2000 call for an intervention in the area of cybercrime.

5. It is necessary to allow the authorities responsible for criminal investigations and prosecutions to have access to traffic data; the legislation of Member States permits in certain cases access to such data in the context of criminal investigations in progress.

6. The retention of traffic data in the absence of a criminal investigation in progress (a priori retention), whether by the telecommunications service providers or by a third party, is technically possible. Many Member States have passed legislation making such a priori retention compulsory for the purpose of criminal investigations or prosecutions. Work in this area is under way in other Member States. The content of this legislation varies considerably.

7. These differences present problems for the provision of telecommunications services beyond the territory of a single Member State and are prejudicial to cooperation in criminal matters. A harmonisation of legislation is therefore desired both by the authorities responsible for criminal investigations and prosecutions and by the providers of telecommunications services.

8. The purpose of this present framework decision is to make compulsory and to harmonise the a priori retention of traffic data in order to enable subsequent access to it, if required, by the competent authorities in the context of a criminal investigation.

9. Such a priori retention of data and access to this data constitutes an interference in the private life of the individual; however, such an interference does not violate the international rules applicable with regard to the right to privacy and the handling of personal data contained, in particular, in the European Convention on the Protection of Human Rights of 4 November 1950, the Convention of the Council of Europe no.108 on the protection of persons in respect of the automated handling of personal data of 28 January 1981, and the Directives 95/46/ce and 97/66/EC, where it is provided for by law and where it is necessary, in a democratic society, for the prosecution of criminal offences.

10. It is necessary to establish certain procedures for the retention of and access to data in order to guarantee their effectiveness and their harmonious application in Member States. These procedures concern the minimum period for the a priori retention of traffic data, the minimum list of types of data that may be retained, and the minimum list of offences for the prosecution of which access to retained data shall be possible.

11. In drawing up other procedures relating to the retention of and access to data, it is important to strike a balance between, on the one hand, the need to allow Member States ample room to make their own individual assessments given the differences that exist between criminal justice systems, and on the other the positive effect of a harmonisation of procedural guarantees for the creation of an area of liberty, security and justice.

12. A period of a minimum of 12 months and a maximum of 24 months for the a priori retention of traffic data is not disproportionate in view of the needs of criminal prosecutions as against the intrusion into privacy that such a retention would entail.

13. The content of the minimum list of types of data to be retained will have an impact on certain sectors, particularly the telecommunications service providers. It is preferable, therefore, that the drawing up of this list of types of data to be retained should be made by further decisions of the Council after the Commission has engaged in the necessary consultations.

14. The drawing up of the minimum list of types of data to be retained must also take into account the invasion of privacy which such a retention entails. Member States must keep this balance in mind should they ever draw up a more extensive list. It should be emphasised that the invasion of privacy would be disproportionate if the data retained related to the content of messages exchanged or of the information sources consulted under whatever form, within the framework of communications.

15. The framework decision would fail in its aim to harmonise procedures for and improve the effectiveness of criminal investigations and prosecutions if access to the retained data were not possible for the prosecution of offences inevitably linked to the use of telecommunications systems or regarded as serious offences in all Member States.

16. The framework decision shall not apply to access to data at the time of transmission, that is by the monitoring, interception or recording of telecommunications.

HAS ADOPTED THE PRESENT DECISION:

Article 1 - Definitions

The following definitions shall apply in this present framework decision

a) "traffic data": all data processed which relate to the routing of a communication by an electronic communications network;[1]

b) "communication": all information exchanged or routed between a finite number of parties via an electronic communications network accessible to the public. [This does not include information routed in the context of a radio service to the public via an electronic communications network except insofar as a link can be established between the information and the subscriber or identifiable user who receives it;[2]

c) "Telecommunications service": services which consist in total or in part of the transmission and routing of signals on telecommunications networks, with the exception of radio and television.[3]

Footnotes:
[1] See article 2, point 2b) of the draft directive of the European Parliament and Council on the handling of personal data and the protection of privacy in the electronic communications sector, (version 15396/2/01 REV 2 ECO 395 CODEC 1375). Initial draft: COM(2000) 385 final - OJ C 365 of 19.12.2000. Article 1 point d) of Convention COE 185 on cybercrime is more specific.
[2] see article 2, point d) of the draft directive (above)
[3] Article 2, point d) of Directive 97/66/CE. Convention COE 185 on cybercrime offers a definition of "service provider".

Article 2 - Access to traffic data

Member States shall take adequate measures to allow the authorities responsible for criminal investigations and prosecutions to have access to the traffic data needed to accomplish their task.

Article 3 - Retention of traffic data and access to data retained

1. The measures envisaged in article 1 include in particular the obligation to retain for the purpose of criminal investigations and prosecutions, either on the part of the telecommunications service provider who holds the data in question, or on the part of a trusted third party, for a period of 12 months minimum and 24 months maximum, the following categories of traffic data:

a) Data necessary to follow and identify the source of a communication;
b) Data necessary to identify the destination of a communication;
c) Data necessary to identify the time of a communication;
d) Data necessary to identify the subscriber;
e) Data necessary to identify the communication device.

2. Each Member State shall take the necessary measure in order to determine with the appropriate precision the exact types of data which must be retained in application of paragraph.1. These types of date shall be limited to what is necessary in a democratic society for criminal investigation and prosecution. These types of data shall not concern the content of the exchanged correspondence or the consulted information, in any form, in the of telecommunications.

3. In implementing paragraph 2, Member States inform each other on the advancement of their work and collaborate with the Commission.

4. The measures envisaged in article 1 shall also include access by the authorities responsible for criminal investigations and prosecutions to data, the retention of which occurred in application of this article. Each Member State determines the offences for the prosecution of which access to traffic data will be possible. In doing so, he makes sure that these offences are sufficiently serious taking into account the limitation of the right to privacy which constitutes this access. He also makes sure that the following offences as defined in national law are at least included:

- offences under the Convention of the Council of Europe no.185 on cybercrime of 23 November 2001;
- participation in a criminal organisation,
- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence, .
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and product piracy,

- forgery of administrative documents and trafficking therein,
- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- motor vehicle crime,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Tribunal,
- unlawful seizure of aircraft/ships,
- sabotage.

Article 4 - Procedural rules and data protection

1. In implementing article 3, Member States take the necessary measure to make sure that:

- Access to retained traffic data is given only to judicial authorities or, in the extent that they have autonomous power in criminal investigation prosecution, to police authorities;

- Access to retained traffic-data is not authorised when other measures are possible which are less intrusive in terms of privacy and leading to similar results regarding criminal investigation and prosecution;

- The process to be followed in order to get access to retained traffic data is defined with precision;

- Confidentiality and integrity of retained traffic data are ensured;

- Data to which access has not been asked at the end of the period of mandatory retention are destroyed;

- Providers of telecommunication services respect the obligation of data retention.

2. Rules mentioned in paragraph 1 are without prejudice to the rules applicable in national law to access to data during their transmission, including tracking, interception and recording of telecommunications.

Article 5 - Obligation to execute a decision of access to retained traffic data

Member States shall undertake to execute, in conformity with this framework decision and on the basis of the principle of mutual recognition, any decision of access to retained traffic data taken by a competent authority of a Member State on the ground of provisions adopted in this Member State in order to implement articles 3 and 4 and transmitted in accordance with article 6 to 8.

Article 6 - Determination of the competent authorities

1. The issuing authority shall be the authority of the issuing State which is competent to issue a decision of access to retained traffic data by virtue of the law of the issuing State.

2. The executing authority shall be judicial authority of the executing State which is competent by virtue of the law of the executing State.

3. Each Member State shall inform the General Secretariat of the Council of the competent authorities under its law.

Article 7 - Transmission of the decision of access to retained traffic data

1. A decision of access to retained traffic data may be transmitted by the issuing authority to the executing authority of a Member State in which the provider of telecommunications services which must have retained the concerned traffic data is located.

2. The decision is accompanied with the following information, in the form of certificate mentioned in paragraph 3:

a) the issuing authority;

b) information allowing to identify the provider of telecommunication services which must have retained the traffic data;

c) the criminal conduct under investigation;

d) indications allowing to select the searched data among all retained data.

3. The Council determines the form of the certificate which will contain information provided for in paragraph 2, taking into account the evolution of the work of the Member States related to the implementation of article 3 paragraph 2.

4. The executing authority may request any further information necessary to enable it to decide whether access to retained data would be authorised in a similar national case.

5. The United Kingdom and Ireland, respectively, may, before the date referred to in Article 9, state in a declaration that the decision of access to retained traffic data together with the certificate must be sent via a central authority or authorities specified by it in the declaration. Any such declaration may be modified by a further declaration or withdrawn any time. Any declaration or withdrawal shall be deposited with the General Secretariat of the Council and notified to the Commission. These Member States may at any time by a further declaration limit the scope of such a declaration for the purpose of giving greater effect to paragraph 1. They shall do so when the provisions on mutual assistance of the Schengen Implementation Convention are put into effect for them.

6. If the competent authority in the executing State is not known to the competent authority in the issuing State, the latter shall make all necessary inquiries, including via the contact points of the European judicial network in order to obtain the information from the executing State.

7. If the issuing authority so wishes, transmission may be via the secure telecommunications system of the European Judicial Network.

8. The issuing authority may forward the decision of access to retained traffic data by any secure means capable of producing written records under conditions allowing the executing Member State to establish its authenticity.

9. All difficulties concerning the transmission or the authenticity of any document needed for the execution of the decision of access to retained traffic data shall be dealt with by direct contacts between the judicial authorities involved, or, where appropriate, with the involvement of the central authorities of the Member States.

10. If the authority which receives a decision of access to retained traffic data is not competent to act upon it, it shall automatically forward it to the competent authority in its Member State and shall inform the issuing authority accordingly.

Article 8 - Conditions of execution

The issuing authority may make the execution subject to conditions which would be applicable in a similar national case.

Article 9 - Implementation

1. Member States shall take the necessary measures to-comply with this Framework Decision by 31 December 2003.

2. They shall communicate to the Council and to the Commission the text of any provisions they adopt to comply with this Framework Decision.

3. The General Secretariat of the Council shall communicate to the Member States and to the Commission the information received pursuant to Article 6 (3) and Article 7 (6). It shall also have the information published in the Official Journal of the European Communities.

Article 10 - Entry into force

This Framework Decision shall enter into force on the twentieth day following its publication in the Official Journal of the European Communities.

Done at Brussels,
For the Council
The President

Questionnaire on traffic data retention

COUNCIL OF THE EUROPEAN UNION Brussels, 14 August 2002

11490/1/02
REV 1

LIMITE

CRIMORG 67
TELECOM 4

from : Presidency
to : Delegations to the Multidisciplinary Group on Organised Crime (MDG)
Subject : Questionnaire on traffic data retention

COVER NOTE

The Presidency, in collaboration with the General Secretariat of the Council, has developed a short questionnaire on traffic data retention that has been attached to this note.

Its objective is to further advance the efforts that are necessary to combat cyber crime and to facilitate the development of strategies and working agendas as they have been laid down *inter alia* in the work programme of the Danish Presidency of the EU for the second half of 2002(footnote).

Delegations are kindly requested to submit their answers (preferably by email) to the General Secretariat of the Council, attention of Mr. Peter Nath, 175 rue de la Loi, B-1048 Brussels, tel.: +32-2-285-6677, facsimile: +32-2-285-8832, email: peter.nath@consilium.eu.int, **no later than Monday, 9th September 2002**.

Questionnaire on Traffic Data Retention

Legislative aspects

1. Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?
2. Has your country yet focussed on a specific period of time for the retention of traffic data? Have you also considered what kind of traffic data should be retained?

3. Has your country considered allowing traffic data retention for purposes other than billing,

such as network security purposes?

Practices and experiences

4. What is the present procedure for a law enforcement authority to obtain traffic data from a service provider? Has this procedure proven to be efficient and effective?

5. Have you received any reports from your law enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?

Dialogue with industry

6. Have you entered into a permanent dialogue with your telecommunications industry about the issue of traffic data retention and what are the tendencies you have observed? How would you judge the general willingness of the telecommunications industry operating in your country to embark on a retention of traffic data?

Perspective

7. How would you rate the solution of creating an instrument on traffic data retention for law enforcement purposes at a European level?

Footnote: Council doc. 10617/02 LIMITE CATS 40.

For further background information and updates please see:

www.statewatch.org/soseurope.htm