COUNCIL OF THE EUROPEAN UNION

Brussels, 28 October 2005

13789/05

LIMITE

COPEN 170
TELECOM 116

NOTE

from :	Presidency
to :	COREPER
No. prev. doc. :	13624/05 COPEN 166 + REV 1
Subject :	Data retention

List of data to be retained.

- **Unsuccessful call attempts and location of mobile equipment**. In relation to both the draft Directive and draft Framework Decision there remains a difference of opinion between delegations as to the proportionality and necessity of retaining data on location of mobile equipment both at the start and end of the communication and / or on unsuccessful call attempts (connected unanswered calls). Decisions need to be taken on whether each of these should be included in the scope of the new instrument or not, and if so whether they should be subject to an extended implementation period. To assist in reaching this decision the Presidency undertook to provide some information on the law enforcement requirements for these types of data. This can be found in Annex I.

- **The technical list of data**: Without prejudice to the outcome of discussions regarding the inclusion of data on unsuccessful call attempts and location of mobile equipment, the Presidency proposes in Annex II the technical list of data to be retained (Article 4 of the draft

Directive to be read in conjunction with Articles 1, 2 and 13). Those elements relevant to unsuccessful calls and location data are in square brackets but reflect the current state of negotiations on the draft Framework Decision (Annex III).

- The Presidency notes that the content of this list would be the same whether it were included in a draft Directive or draft Framework Decision. As discussed in COREPER on 25 October, Member States could require in accordance with Article 15(1) of the 2002 Telecomms Directive the retention of other types of data not falling on the list. This is clarified further by the new Recital 12bis.

- **Definitions**: At the Article 36 Committee on 19 October several delegations noted that the scope of the technical list of data to be retained was linked to the definitions of certain types of data. Others also saw a link with the issue of whether companies should be obliged to keep data which was "generated or processed" or "generated and processed". Suggested amendments to Articles 1 and 2 of the draft Directive reflect the current state of negotiation on these points.

- **Status**: As proposed at the October JHA Council, the revised text of Article 4 of the draft Directive now proposes that the list be fixed within the body of the new instrument, subject to a review clause in Article 12. The review would be informed by, amongst other things, the collection of statistics proposed in Article 9 of the draft Directive. This approach would require the deletion of the comitology arrangements in the draft Directive.

Engagement with the European Parliament

The October JHA Council concluded that work should continue on both the draft Directive and draft Framework Decision with a view to reaching a final decision at the December JHA Council. If the Council decides to work for a final agreement on the draft Directive in December, it will only be in a position to do so on the basis of an agreed text with the European Parliament.

Having made progress within COREPER on key issues of substance the Presidency will now, with the Commission, take forward discussions with the EP in order to maximise common ground between the institutions, in line with the JHA Council's conclusions.

The Presidency notes that these discussions will take place without prejudice to the decision to be taken by the Council on the appropriate legal base and to ongoing negotiations in COREPER.

On that basis, the Presidency, with the Commission, intends to meet with European Parliament representatives on 8 November to discuss possible draft amendments to the Directive. The Presidency will report back on the outcome of those discussions to COREPER on 9 November.

ANNEX I: Unsuccessful call attempts and location data

Call location data

(i) What is call location data?

A caller's geographical location can be identified by data showing which telephone mast (Cell ID) was used to relay the call. Mobile phone networks generate this data which is fundamental to the operation of a mobile phone network, for example in identifying whether a call is made using a home network or is roaming. But because telephone masts may be re-labelled or re-named over time as new ones are installed it is also necessary to keep a historic 'map' of their location to ensure that the correct mast, and therefore the right location, can be identified months after the call took place. Those maps are what is meant by "data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained."

(ii) Law enforcement need

Knowledge of the location from which a call was made at any given time has repeatedly proven its value in criminal investigations and prosecutions:

- A conviction in a case involving the murder of two young girls was based partly on mobile phone evidence. Mobile phone data helped to disprove the suspect's alibi as it showed that his girlfriend's phone was in another town when she had told police that she was with him. This evidence was based on analysis of the cell phone masts to which her phone was connected.

- Location data can also be used to exonerate suspects. In April 2002, two brothers aged 16 were cleared of murdering a 10-year-old boy. The judge ruled that they could not have run from where he sustained his fatal injury to an area where they made mobile calls shortly afterwards.

- In Northern Ireland, mobile phone location data was vitally important in pinpointing the positions of those involved in the Omagh bombing which resulted in the deaths of 29 people. The pattern of calls and connections to cell-masts showed that the accused had been located at the point of the bomb's origin and also in Omagh shortly before its detonation.

(iii) Impact on business

Mobile companies generate and retain cell data records which include location information so that they can conduct analysis to look at the network volumes, pricing tariffs (reduced rate when "near to home"), fraud management & prevention (e.g. illicit GSM gateways, dial-through fraud or illegal call centres).

Unsuccessful calls attempts

(i) Law enforcement need

Data on unsuccessful (unanswered) call attempts is regularly used during investigations into crimes such as murder, drug trafficking and terrorism. In particular such calls can be used as a signal to an accomplice or as a way of detonating explosives. Equally, they have been used to prove a person's innocence.

- Following the kidnap and subsequent murder of a family, police were able to establish the time and date that the wife, two children and her mother had been abducted by looking at the pattern of phone records from the landline at her home. These showed that, following the husband's earlier abduction, the wife had repeatedly called his mobile number from the landline at her home without getting any reply. After 12:59 on Saturday, 15 February 2003, the landline was never used again. Location data from the husband's mobile phone records provided a link to one of the murderers by demonstrating to the police that he had been held captive where one of his murderers lived. Three men were convicted of murder in July 2005 after a two-year inquiry involving thousands of police officers and a £10m eight-month trial.

- In Manchester, a woman was murdered in her home. Routine enquiries were made into the incoming and outgoing calls made before her murder. Unsuccessful call data indicated she made an outgoing call that was not answered, with the inference she was still alive and well. Later still were a series of incoming unanswered calls, with the inference she was dead. The unsuccessful call data greatly assisted to narrow the time window of the murder investigation.

- A paedophile was kidnapped by a group of young male prostitutes and taken to a flat they used for their business, where they unintentionally beat him to death. In a panic about what to do with the body they bombarded the owner of the flat with phone calls. Unable to contact the owner, they used the dead man's credit card to buy a fridge to store the body. Use of the credit card and CCTV footage helped police identify the flat containing the fridge and body and the flat's owner was subsequently arrested. Truthfully he claimed to know nothing of the events. His call records indicated that he was elsewhere at the time, but a significant number of connected unanswered calls led police to identify mobile phones used by the killers, and identify, arrest and subsequent convict them.

(ii) Impact on business

If telecoms companies do not already retain such data there would be additional costs associated with an obligation to do so. However, the cost per call of retaining connected unsuccessful calls is no greater than that of retaining connected successful calls. Some telephone companies find there is a commercial interest in retaining this data since it provides evidence for them to demonstrate to their corporate customers that they need extra telephone lines to meet their business needs. This data is also used for monitoring the volume of unsuccessful calls to and from call centres (eg direct sales) and in other businesses that rely on telephone based work.

ANNEX II: Proposed amendments to the draft Directive as in 12671/05 COPEN 150

Those provisions not reproduced here remain unchanged. This is without prejudice to further changes that may be required on other outstanding issues.

Article 1

Subject matter and scope

1. This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the … retention of certain data <u>which are generated or processed</u> by such providers, in order to ensure that the data is available for the purpose of the …, investigation, detection and prosecution of … criminal offences …...

Article 2

Definitions

2. For the purpose of this Directive:

(c) the term “telephone service” means calls (including voice, voicemail, conference or data), supplementary services (including call forwarding and call transfer), messaging and multi-media services (including Short Message Services, Enhanced Media Services and Multi-Media Services);

(d) the term “User ID” means an unique identifier located to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;

(e) [the term “Cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated];

(f) [the term "unsuccessful call attempt” means a communication in a which a telephone call has been successfully connected but is unanswered or there has been a network management intervention.]

Article 3

Obligation to retain data

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation…..

Article 4

Categories of data to be retained

Member States shall ensure that the following categories of data are retained under this Directive:

a) Data necessary to trace and identify the source of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) …

(3) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The User ID(s) allocated.

(b) The User ID and telephone number allocated to any communication entering the public telephone network.

(c) Name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, …User ID or telephone number was allocated at the time of the communication.

b) Data necessary to identify the destination of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The number(s) dialled (the called telephone number or numbers), and in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed.

(b) Name(s) and address(es) of the subscriber(s) or registered user(s).

(2) …

(3) Concerning …Internet e-mail and Internet telephony:

(a) The … User ID or telephone number of the intended recipient(s) of an Internet telephony call.

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) and User ID of the intended recipient of the communication.

c) Data necessary to identify the date, time and duration of a communication.

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access …:

(a) The date and time of the log-in and log-off of the Internet Access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication, and the User ID of the subscriber or registered user.

(3) Concerning Internet e-mail and Internet telephony:

(a) The date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service based on a certain time zone.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The telephone service used ….

(2) Concerning Internet e-mail and Internet telephony

(a) The Internet service used.

e) Data necessary to identify users' communication equipment or what purports to be their equipment.

(1) Concerning Fixed Network Telephony

(a) The calling and called telephone numbers.

(2) Concerning Mobile Telephony

(a) The calling and called telephone numbers.

(b) The International Mobile Subscriber Identity (IMSI) of the calling party.

(c) The International Mobile Equipment Identity (IMEI) of the calling party.

(d) The International Mobile Subscriber Identity (IMSI) of the called party.

(e) The International Mobile Equipment Identity (IMEI) of the called party.

(f) In case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the activation was made.

(3) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The asymmetric digital subscriber line (ADSL) or other end point ….. of the originator of the communication.

(c) The media access control (MAC) address or other machine identifier of the originator of the communication.

[f). Data necessary to identify the location of mobile equipment.

(1) The location label (Cell ID) at the start … of the communication.

(2) The location label (Cell ID) at the end of the communication.

(3) Data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained.]

Article 5

Revision of the annex

….[deleted]

Article 6

Committee

….[deleted]

Article 7

Periods of retention

Member States shall ensure that the categories of data referred to in Article 4 are retained for periods of not less than 6 months and for a maximum of two years from the date of the communication….. *[remainder deleted]*

Article 10

Costs

….[deleted]

Article 11

Amendment of Directive 2002/58/EC

In Article 15 of Directive 2002/58/EC a paragraph 1a is inserted, as follows:

"1a. Paragraph 1 does not apply to the retention of data mentioned in Article [4] of Directive 2005/…../EC for the purposes referred to in Article 1(1) of that Directive".

New Article X

Future measures

1. A Member State facing particular circumstances warranting an extension for a limited period of the maximum retention period referred to in Article 7 may take the necessary urgent measures. The Member State shall immediately notify the Commission and inform the other Member States of the measures taken by virtue of this Article and indicate the grounds for introducing them.

2. The Commission shall, within six months after the notification as referred to in paragraph 1, approve or reject the national measures involved after having verified whether or not they are a means of arbitrary discrimination or disguised restriction of trade between Member States and whether or not they shall constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

3. When, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may examine whether to propose an adaptation of this Directive.

Article 12

Evaluation

1. Not later than three years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the list of data in Article 4 and the periods of retention provided for in Article 7.

Article 13

Transposition

[3. Each Member State may for a period of up to two years from the expiry of the deadline referred to in paragraph 1 defer from its application of this Directive the retention of communications data relating to any or all of the following communication data:

(a) unsuccessful call attempts on Fixed Network Telephony or Mobile Telephony;

(b) Internet Access, Internet telephony and Internet email.

Any Member State which intends to make use of this paragraph shall, by way of a declaration, notify the Commission to that effect upon adoption of this Directive. The declaration shall be published in the Official Journal of the European Union.]

Annex

….*[deleted]*

Recitals

9bis In an area of freedom, security and justice, obligations upon Industry to retain data are justifiable only if necessary to preserve important interests within a democratic society. This necessity arises from the importance of analysing specific historic data in the investigation, detection and prosecution of terrorist crimes and other serious offences. Where that data may provide the only approach for an effective resolution of such crimes, its availability for a determined period of time may be reliably ensured only with a statutory storage obligation.

(11) Given the importance of traffic data for the … investigation, detection, and prosecution of … criminal offences ….., as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.

(12) …..[*deleted*]

(12bis) Article 15(1) of Directive 2002/58/EC would continue to apply in relation to types of data falling outside the scope of this Directive and for retention for purposes other than those covered by this Directive.

(13) ….. [*deleted*]

(17) …. [*deleted*]

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the … investigation, detection and prosecution of …. criminal offences …., cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

ANNEX III

Draft Framework Decision

on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of investigation, detection and prosecution of crime and criminal offences including terrorism.

The text has been duplicated here from 12894/1/05 COPEN 153 REV 1 insofar as it relates to the issues in the covering paper. Changes to Article 3 reflect discussions in the Article 36 Committee on 19 October and work to align the list with that proposed for the draft Directive.

Article 1

Scope and Aim

1. This Framework Decision aims to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of communication data, generated or processed by providers of a publicly available electronic communications service or a public communications network, for the purpose of investigation, detection and prosecution of criminal offences.

3. This Framework Decision is without prejudice to:

- national rules on retention of communication data processed or generated by providers of a publicly available electronic communications service or a public communications network for the purpose of prevention of crime;
- (..…)
- the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;
- the rules applicable to the exchange of information within the framework of police and customs co-operation;
- activities concerning public security, defence and national security (i.e. State security).

Article 2

Definitions

For the purpose of this Framework Decision,

1. the term "communication data" means:

   (a) traffic data and location data as defined in Article 2 of the Directive 2002/58/EC;

   (b) user data, which means data relating to any natural or legal person using a publicly available electronic communications service, for private or business purposes, without the user necessarily having subscribed to the service;

   (c) subscriber data, which means data relating to any natural or legal person subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

2. ….

3. the term “telephone service” means calls (including voice, voicemail, conference or data), supplementary services (including call forwarding and call transfer), messaging and multi-media services (including Short Message Services, Enhanced Media Services and Multi-Media Services);

4. the term “User ID” means an unique identifier located to a person as they subscribe or register to an Internet Access Service or Internet Communication Service;

5. [the term “Cell ID” means the identity of the cell from which a mobile telephony call originated or in which it terminated];

6. [the term "unsuccessful call attempt” means a communication in a which a telephone call has been successfully connected but is unanswered or there has been a network management intervention].

Article 3

Retention of communication data

1. Each Member State shall take the necessary measures to ensure that, for the purpose set out in Article 1, at least the following communication data are retained to the extent it is generated or processed by providers of a publicly available electronic communications service or a public communications network in the process of supplying the communication services concerned:–

a) Data necessary to trace and identify the source of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) …

(3) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The User ID(s) allocated.

(b) The User ID and telephone number allocated to any communication entering the public telephone network.

(c) Name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, User ID or telephone number was allocated at the time of the communication.

b) Data necessary to identify the destination of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The number(s) dialled (the called telephone number or numbers), and in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed.

(b) Name(s) and address(es) of the subscriber(s) or registered user(s).

(2) …

(3) Concerning Internet e-mail and Internet telephony:

(a) The User ID or telephone number of the intended recipient(s) of an Internet telephony call.

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) and User ID of the intended recipient of the communication.

c) Data necessary to identify the date, time and duration of a communication.

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access:

(a) The date and time of the log-in and log-off of the Internet Access service based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet Access Service provider to a communication, and the User ID of the subscriber or registered user.

(3) Concerning Internet e-mail and Internet telephony:

(a) The date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service based on a certain time zone

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony

(a) The telephone service used.

(2) Concerning Internet e-mail and Internet telephony

(a) The Internet ..… service used.

e) Data necessary to identify users' communication equipment or what purports to be their equipment.

(1) Concerning Fixed Network Telephony

(a) The calling and called telephone numbers.

(2) Concerning Mobile Telephony

(a) The calling and called telephone numbers.

(b) The International Mobile Subscriber Identity (IMSI) of the calling party.

(c) The International Mobile Equipment Identity (IMEI) of the calling party.

(d) The International Mobile Subscriber Identity (IMSI) of the called party.

(e) The International Mobile Equipment Identity (IMEI) of the called party.

(f) In case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the activation was made.

(3) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The asymmetric digital subscriber line (ADSL) or other end point …. of the originator of the communication.

(c) The media access control (MAC) address or other machine identifier of the originator of the communication.

[f). Data necessary to identify the location of mobile equipment.

(1) The location label (Cell ID) at the start of the communication.

(2) The location label (Cell ID) at the end of the communication.

(3) Data identifying …the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained.]

Article 4

Time periods for retention of communication data

1. Each Member State shall take the necessary measures to ensure that communication data referred to in Article 3 shall be retained for a period of 12 months following its generation. Relating to subscriber data, this period shall run from the end of the subscription.

2. By derogation from paragraph 1, any Member State may provide for retention of communication data referred to in Article 3 for longer periods of up to 48 months in accordance with national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

3. By derogation from paragraph 1, any Member State may provide for retention of communication data referred to in Article 3 for shorter periods of at least 6 months should the Member State not find acceptable, following national procedural or consultative processes, the retention period set out in paragraph 1 of this Article.

4. Any Member State which decides to make use of paragraphs 2 or 3 must notify the Council and the Commission of the retention periods provided for with specification of the communication data concerned. Any such derogation must be reviewed at least every 5 years.

Article 5

Data security and data protection

Each Member State shall ensure that communication data retained under this Framework Decision is subject, as a minimum, to the rules implementing Article 17 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movements of such data, to the provisions of Article 4 of Directive 2002/58/EC and the following data security principles:

(a) the retained data shall be of the same quality and shall be subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised or unlawful disclosure or access, and against all other unlawful forms of processing;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that disclosure of, and access to, the data is undertaken only by authorised persons whose conduct is subject to oversight by a competent judicial or administrative authority;

(d) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved.

Article 6

Access to retained communication data

Each Member State shall ensure that access for the purposes referred to in Article 1 to communication data retained under this Framework Decision shall be subject, as a minimum, to the following rules and shall establish judicial remedies in line with the provisions of Chapter III on 'Judicial remedies, liability and sanctions' of Directive 95/46/EC:

(a) data shall be accessed for specified, explicit and legitimate purposes by competent authorities on a case by case basis in accordance with national law and not further processed in a way incompatible with those purposes;

(b) the process to be followed and the conditions to be fulfilled in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law;

(c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are accessed. Data shall be processed fairly and lawfully;

(d) data accessed by competent authorities shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected or for which they are further processed;

(e) the confidentiality and integrity of the data shall be ensured;

(f) data accessed shall be accurate and, every necessary step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

Article 8

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision within two years of its entry into force.

2. By the same date Member States shall transmit the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. The General Secretariat of the Council shall communicate to the Member States the information received pursuant to this Article.

3. Each Member State may for a period of up to two years from the expiry of the deadline referred to in paragraph 1 defer from its application of this Framework Decision the retention of communications data relating to any or all of the following communication data:…:

(a) unsuccessful call attempts on Fixed Network Telephony or Mobile Telephony;

(b) Enhanced Media Services and Multi-Media Services on Fixed Network Telephony or Mobile Telephony;

(c) Internet Access and Internet Communication Services.

Any Member State which intends to make use of this paragraph shall, by way of a declaration, notify the General Secretariat of the Council to that effect upon adoption of this Framework Decision. The declaration shall be published in the Official Journal of the European Union.

4. The Commission shall by [1st January 2008] submit a report to the Council assessing the extent to which the Member States have taken necessary measures in order to comply with this Framework Decision. The Council shall thereafter review the list of data to be retained in particular with reference to the possibility of including additional types of Internet data.

Recitals

1. Offering a high level of protection in an area of liberty, security and justice requires that the investigation, detection and prosecution of crime and criminal offences be carried out in an efficient and effective manner which respects the fundamental human rights of individuals.

7. In recognition of the importance of the need to retain data, Article 15 of Directive 2002/58/EC permits the adoption of legislative measures allowing, under certain conditions, retention of data for the purposes of the prevention, investigation, detection or prosecution of crime and criminal offences. This Framework Decision is not related to other objectives set out in Article 15 of this Directive and therefore does not provide for rules on data retention for the purpose of safeguarding national security (i.e. State Security), defence and public security. Nor is it related to the unauthorised use of the electronic communication system when such use does not constitute a criminal offence.

9bis In an area of freedom, security and justice, obligations upon Industry to retain data are justifiable only if necessary to preserve important interests within a democratic society. This necessity arises from the importance of analysing specific historic data in the investigation, detection and prosecution of terrorist crimes and other serious offences. Where that data may provide the only approach for an effective resolution of such crimes, its availability for a determined period of time may be reliably ensured only with a statutory storage obligation.

12. Data may be a priori retained for different periods of time depending on its type. The retention periods for each type of data will be dependant on the usefulness of the data in relation to the investigation, detection, and prosecution of crime and criminal offences and the cost of retaining the data. The retention periods shall be proportionate in view of the needs for such data for the purposes of investigating, detecting and prosecuting crime and criminal offences as against the intrusion into privacy that such retention will entail from disclosure of that retained data.

13. The drawing up of any lists of the types of data to be retained must reflect a balance between the benefit to the investigation, detection, and prosecution of crime and criminal offences of keeping each type of data against the level of invasion of privacy which will result.

15. Member States must ensure that access to retained data takes account of privacy rules as defined in international law applicable to the protection of personal data.

16. Recognising that the retention of data no longer required for business purposes can represent practical and financial burdens upon Industry, Member States should ensure that implementation of this Framework Decision involves appropriate consultation with Industry with particular regard to the practicality and cost of retaining that data.

_____