Technical Questions on Data Retention

1) The list of data in the annex of the proposed Directive on Data retention is practically identical to the information required in the Council draft Framework Decision. Why have these particular sets of data been singled out in the proposal?

   Answer:

   The choice for these particular sets of data has been based on long discussions within the Council Working Groups, consultation with law enforcement experts and industry. They represent what could be called the essential elements for the effectiveness of the proposal, and reflect those datasets most often required and used by law enforcement authorities to identify who has been in contact with whom, using what means, and at what time.

2) Most of us are not IT experts. Can you explain what each of these sets of data actually mean in layman's terms, and why this data is vital to store (or can a detailed written explanation be prepared for us), i.e. connection label?

   Answer:

   Most of the datasets related to fixed and mobile telephony are easy to understand (numbers used, addresses of users/subscribers etc.). Perhaps the most questions are raised with respect to technical data related to mobile phones, such as IMSI, IMEI and data mapping between Cell ID and location data. Also, questions could be raised with respect to the datasets required for internet usage. This answer focuses on these more technical categories of data.

   IMSI: International Mobile Subscriber Identifier. A unique 15-digit number which designates the subscriber. This number is used for provisioning in network elements. The IMSI number is stored on the SIM card, so it does not change if SIM cards are exchanged between mobile phones.

   IMEI: International Mobile Equipment Identifier. A unique 15-digit number that serves as the serial number of the GSM handset. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults.

   Cell ID: A Cell is the basic geographic unit of a cellular system. Also, the basis for the generic industry term: "cellular." A city or county is divided into smaller "cells," each of which is equipped with a low-powered radio transmitter/receiver. The cells can vary in size depending upon terrain, capacity demands, etc. By controlling the transmission power, the radio frequencies assigned to one cell can be limited to the boundaries of that cell. When a wireless phone moves from one cell toward another, a computer at the Mobile Telephone Switching Office (MTSO) monitors the movement and at the proper

time, transfers or hands off the phone call to the new cell and another radio frequency. The handoff is performed so quickly that it is not noticeable to the callers. Cell ID is the identification of each Cell.

Data mapping between Cell IDs and their geographical location at the start and end of the communication: Given the fact that cell ID's may change over the period of retention, this category of data would require operators to store data which allows them to identify the location of a particular cell at the time when a call is made. Without such mapping, if changes had occurred in the assignment of Cell ID between the time the call was made and the data are requested, it would be impossible to identify the location from which the call was made with certainty. This particular data set, often misunderstood, does not cover location data during the communication, nor does it allow for the creation of so-called "movement profiles" of users.

Connection label: any data which is used as an alternative to a telephone number when IP telephony is concerned. Instead of a normal number, such connection labels may consist of letters or other designators/identifiers of the connection which is being sought. In ISDN telephony, the term *connection identification code* is also used.

User ID: a User ID is usually associated with internet access and allows the identification of the user when connecting to the internet.

The media access control (MAC) address: number assigned for example to a cable modem supplied by some Internet Service Providers. Allows for the identification of users through identification of the modem used to access the internet.

3) How will retaining this data help to track data flows from someone who uses a false identity, logs onto different computers, creates new email accounts on each occasion etc? And how can we be sure that this data will actually tell us the identity of the author of these data flows. For example, a computer can have multiple users, mobile phones can be lent to friends or be stolen. The retained data may wrongly give us the impression that someone is connected to a crime or terrorist activity when in fact they are not. If a terrorist orders a pizza by telephone does the pizza delivery man become a suspect?

Answer:

Even if someone uses a false identity, part of the datasets to be retained will be useful in any case. For example, the location data of mobile phones is independent of identity. This is also true for IP addresses to some extent – the IP address will allow the identification of a communication to a particular PC used, and in the case of fixed equipment, also to the identification of the telephone number used to connect to the internet. In such cases the actual address from which the communication has taken place can be identified. This is also the case if someone uses different computers. Creation of new e-mail accounts will also not be a problem in such scenarios, given that the IP address from which the e-mail was sent will be the decisive factor in identification.

Obviously this does not always lead to an immediate identification of the user. However, **such data is indispensable to allow for further investigations to take place.** In general, traffic data is mostly used to identify links between individuals, which then need to be investigated further to see whether they are relevant to the on-going investigation. It is clear that the mere fact that a suspected terrorist has dialled a certain number does not mean that the person contacted is in fact associated with any terrorist activity. However, analysis of the traffic data obtained is usually a key indicator of which numbers need to be investigated. For example, numbers called more often provide more indications of regular contacts, which are more likely to be significant to the investigation. Traffic data are thus more relevant to provide for clues to the law enforcement authorities, than to provide for actual evidence (either incriminating or exculpating) directly related to a crime.

4) Ireland and Italy already have laws requiring data to be stored. What types of data do they require to be stored? Is it very different data to what is proposed in the Directive? Is it more or less?

   Answer:

   Both Ireland and Italy require telephone data (both fixed and mobile) to be stored for long periods (3 and 4 years respectively). Additionally, in the case of Italy, internet data must be retained for a period of 1 year.

5) Who will be the competent authorities in the Member States, and who decides?

   Answer:

   Under the Commission's proposal, it is the Member States themselves which determine which authorities are competent to access the data. This is primarily due to two points. Firstly, there are many different authorities in the different Member States which deal with the prevention and combating of serious crime. Such authorities also have different mandates. Secondly, the legal basis chosen for the instrument does not allow such authorities to be identified at the EU-level.

6) Will the authorities need a warrant to search the retained information?

   Answer:

   That will depend on the national legislation of the Member State involved. Different choices, with different applicable safeguards, can be made by the Member States within the limits set by the Directive.

7) Who has access to the information that is stored? Are Member States allowed to exchange data between themselves?

   Answer:

See firstly the answer to question 6. In addition, the Commission's proposal is that only those authorities which are competent for preventing and combating serious crime should have access to the data. The wording of Article 3 (2) on this issue reads: "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, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime." As soon as the data are lawfully accessed by law enforcement authorities, and are processed by them, they are not treated differently than other data held by such authorities. This means that the normally applicable instruments for police and judicial co-operation determine whether or not the data can be exchanged with other Member States.

8) Will there be a 'push' or 'pull' system? Will authorities be able to have direct access, or will the requested data be 'pushed' to them?

Answer:

The question whether a pull or push system should be used is not addressed by the Commission's proposal. However, logic dictates that a "push" system is less likely, given the fact that the proposal foresees that data may only be provided on a case-by-case basis. A "push" system would thus only make sense with respect to data related to pre-identified individuals (a request to provide for all traffic data related to a particular person).

9) How will it be ensured that the companies themselves do not access this stored data for their own purposes, or sell it on to third parties, since this data will be very valuable.

Answer:

Under Article 3 (2) of the proposal, the data may only be provided to the competent authorities of the Member States. Selling the data to third parties is thus prohibited. Use of the data for the own purposes of the companies themselves is limited by the fact that Directive 2002/58 is directly applicable to such data. That Directive prescribes in detail what use companies may make of the data under their control.

10) Will the companies be allowed access to anonymised data, and will they be able to sell this?

Answer:

See the answer to question 9. Although the issue of anonymised data is not addressed directly in the proposal, the restriction of Article 3 (2) is not limited to personal data – it applies to all traffic data. This would imply that it also applies to such data in an anonymised form.

11) Which set of standards are actually applied by the EU Service providers and which kind of standards could be proposed/imposed to ensure a strong physical and logical protection of data ?

Answer:

It is not possible to provide for a complete set of standards which are actually applied by the EU Service providers. However, all these standards must meet the requirements of both Directives 95/46 and 2002/58. One should not forget that these standards were established with even the most confidential data in mind – such as medical or financial data. It seems difficult to create specific standards for each specific set or category of data.

12) Would it be possible/advisable for the ENISA Agency to play a role for improving the security of data ?

Answer:

Under Article 1 of the ENISA regulation (OJ L77/1, 13.3.2004), its task is to "assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security". Although it therefore is not set up to provide direct advise to individual companies, its advice to the Commission and the Member States may well be of significance to improving the security of data. For example, Article 3 (e) provides that one of the tasks of ENISA is to "contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, *inter alia*, promoting exchanges of current best practices, including on methods of alerting users (…)".

13) In case of misuse of data or illicit access from unauthorised persons which are (if they exists) and which nature (penal/administrative) the sanctions in MSs?

Answer:

The issue of penal/administrative sanctions is addressed in three different EU instruments. Firstly, the Framework Decision on Attacks against Information Systems should be mentioned. This FD was adopted in March 2005, and prescribes that the MS must provide for effective, proportional and dissuasive criminal penalties for illegal access to information systems, illegal system interference and illegal data interference. Secondly, Chapter III of Directive 95/46 contains obligations for Member States to provide for judicial remedies, liability of the controller of the data and also sanctions to be imposed in case of infringement of the provisions of that Directive. Thirdly, by virtue of Article 15 (2) of Directive 2002 (58), these provisions are equally applicable to data protection in the telecommunications sector. At this stage there is no complete overview how these obligations have been implemented by all Member States.

14) Third Countries such as the US may be very interested in the data that will be stored. Will they have access to this data? In the case of PNR the US simply passed a law that granted it direct access to airlines' databases. A similar danger would exist for these mountains of stored data ?

Answer:

Firstly, reference is made to the answer to question 7. As soon as data has been obtained from the service providers and is processed by the competent law enforcement authorities, these data are covered by the national legislation applicable (e.g. data protection and code of criminal procedure). National legislation on data protection will be harmonised through the FD on data protection which the Commission has recently proposed. That FD also deals with the issue of providing personal data to third States – with one of the conditions being that an adequate level of data protection needs to be ensured in that third State. In addition, the normal legal instruments for providing police or judicial co-operation will be fully applicable. This may include bi-lateral treaties, but also multi-lateral treaties such as the Cybercrime Convention. The exchange of traffic data is thus no different than the exchange of other data. The comparison with PNR is not applicable, in the sense that the US can not impose a legal obligation to access all such data. In the PNR case, the situation is different given the fact that the obligation to supply the data was legislated as a condition on flying to the US.

15) Will it be possible for members of the public to make subject access requests? How will they know which company to turn to, or which company is holding information on them? People have a right to know if information is being stored about them.

Answer:

The right to have access to information stored is indeed one of the main principles of data protection legislation. Given the fact that Directives 95/46 and 2002/58 will be fully applicable to the data processed, rights of access, correction and deletion are fully applicable to the data retained. Individuals will know which company to turn to on the basis of the relationship they have with the company providing the communication service to them.

16) There are some extraterritorial dimensions to the proposed Directive. Will it apply in practice to a firm based solely in a third country (such as a firm operating Voice over Internet Protocol services) but providing services by way of the internet in the EU? Will they also have to store data?

Answer:

No. Article 3 (1) of the proposal limits the obligations which must be imposed by Member States to those companies which are within their jurisdiction. This excludes companied based solely in a third country. However, in those cases where the VOIP services include communications entering into the normal telephony networks in the EU, such data would be retained by the network operators within the EU.

17) If states were to reimburse firms for extra costs, how would these firms demonstrate the extra costs? Which Member State would pay these costs? If a firm from Luxembourg operates mostly in Germany and has to store data on Millions of Germans, which government should pay these extra costs?

Answer:

The details of the reimbursement schemes which MS would need to set up under the Commission's proposal are not dealt with within that proposal itself. Member States will thus have some flexibility in how they implement the principle of reimbursement.

18) Can we have some clarification on the purpose of storing the data? Will it be used, like after the London bombings, for retracing the movement of known terrorists, or will it be used for tracking suspected terrorists or criminals before they strike? Will it be used to catch petty criminals? Will everyone be monitored? What safeguards are in place to make sure the EU does not become a police state?

Answer:

The purpose for storing the data is explicitly laid down in Article 3 (2) of the proposal: the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. This means that it can indeed be used for retracing the movements of known terrorists, but can also be used for tracking suspected terrorists or criminals before they strike. It is therefore important that the data may also be used for prevention. Given the purpose limitation, the data may not be used to catch petty criminals. Even though traffic data will be retained on everyone who uses communication services, the purpose limitation means that only those data which are of relevance to the purposes established will actually end up under the control of the law enforcement authorities. The largest majority of data retained will need to be destroyed after the retention periods have expired.

19) Concerning the category of data necessary to identify **the destination** of a communication, should the telecom provider of the caller collect these data? if so, is it technically possible for a telecom provider to obtain the name and address of the user/subscriber of the number that is called (which could be administered by a different company)? E.g. if a Vodafone user calls a Base user, should Vodafone retain the name and address of the Base user? How does this work in case of international calls?

Answer:

Considering that the obligations on providers of electronic communications services should be proportionate, the Directive requires that they only retain such data which are generated or processed in the process of supplying their communications services. The categories of data to be retained shall therefore not go beyond the data which they generate or process within their own systems. It is not normally possible for a telecommunications provider to obtain the name and address of the user/subscriber of

the called party, if that called party is not one of its own subscribers or users. However, it is possible for the telecommunications providers to know the number called – such information would need to be retained, so that the competent authorities can then require further information from the company which has given out that number to one of its subscribers.

20) Art. 20 of the Cybercrime Convention foresee the "preservation" of data and art. 29 WG suggests to have a "quick freeze" system; how could these methods complement the retention/system ?

Answer:

The data retention scheme is a necessary complement to the system of “preservation of data” foreseen by the Cybercrime Convention. As states in the Impact Assessment document (page 12) “In fact, data preservation is a very useful tool for law enforcement authorities. Undoubtedly, in those cases where a suspect has been identified, or where an investigation into for example an organised crime group or terrorism cell is underway, requests for preservation of traffic data are an indispensable tool to establish the connections between suspects and their contacts and associates. At the same time, the logical limitations of this approach can be easily explained – with only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects.”

21) In case of large WI-FI project covering villages and even large town how data will be collected, stored, protected ?

Answer:

In those cases where public Internet Access is provided without further requirements with respect to costs or user identification, the data to be retained will be limited to the IP addresses assigned to the internet connections used to make use of the WIFI connection to access the internet. Although it will not be possible in those cases to actually identify the user, it will give indications as to the location from which the communication was made – which can provide valuable clues to law enforcement.