Brussels, 29 October, 2001

EU FORUM ON CYBERCRIME

Discussion Paper for Expert's Meeting on Retention of Traffic Data
6 November 2001

Please note : This is an informal Working Paper prepared by the Commission services (Directorate-General for Justice and Home Affairs, and the Directorate-General for the Information Society).

1. INTRODUCTION

The Cybercrime Communication[1] presented the position of the Commission with respect to the general issue of data retention by network operators and service providers. This issue is a sensitive one, with strong arguments supporting the different opinions expressed.

The Cybercrime Communication argued in favour of a balanced approach that would be consensus based and that was the result of a broad consultation through an EU-Forum on Cybercrime that the Communication envisaged. The first section of this paper takes over the relevant paragraphs of the Cybercrime Communication dealing with the retention of traffic data.

The second section asks questions related to the issue of traffic data. Experts will be invited to respond to these questions at the expert meeting, in order to enrich the knowledge of the Commission on the industry and law enforcement practices related to traffic data retention and the relevant data protection aspects.

Annexes I and II to the present document provide for an overview of business and technology-related issues related to data generated by electronic communications.

This paper should therefore not be interpreted as reflecting the position of the European Commission.

2. RETENTION OF TRAFFIC DATA

To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. As the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.

[1] See Annex on relevant documents

In accordance with the EU personal Data Protection Directives, both the general purpose-limitation principles of Directive 95/46/EC and the more specific provisions of Directive 97/66/EC, traffic data must be erased or made anonymous immediately after the telecommunications service is provided, unless they are necessary for billing purposes. For flat rate or free-of-charge access to telecommunications services, service providers are in principle not allowed to preserve traffic data.

Under the EU Data Protection Directives, Member States may adopt legislative measures to restrict the scope of the obligation to erase traffic data when this constitutes a necessary measure for, amongst others, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.

However, any legislative measure at national level that may provide for the retention of traffic data for law enforcement purposes would need to fulfil certain conditions: the proposed measures need to be appropriate, necessary and proportionate, as required by Community law and international law, including Directive 97/66/EC and 95/46/EC, the European Convention for the Protection of Human Rights of 4 November 1950 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981. This is particularly relevant for measures that would involve the routine retention of data on a large part of the population.

Some Member States are taking legal initiatives requiring or allowing service providers to store certain categories of traffic data, not needed for billing purposes, after the provision of the service but which are considered useful for criminal investigations.

The scope and form of these initiatives varies considerably, but they are all based on the idea that more data should be available for law enforcement authorities than would be the case if service providers only process data which are strictly needed for the provision of the service. The Commission is examining these measures in the light of existing Community law.

The European Parliament is sensitive to privacy issues and generally has taken a stance in favour of strong protection of personal data. However, in discussions on combating child pornography on the Internet, the European Parliament has expressed an opinion favouring a general obligation to preserve traffic data for a period of three months.

This illustrates the importance of the context in which a sensitive topic such as traffic data retention is discussed and the challenge facing policy makers seeking to strike appropriate balances.

The Commission considers that any solution on the complex issue of retention of traffic data should be well founded, proportionate and achieve a fair balance between the different interests at stake. Only an approach that brings together the expertise and capacities of government, industry, data protection supervisory authorities and users will succeed in meeting such goals. A consistent approach in all Member States *on this complex issue would be highly desirable, to meet the objectives of both effectiveness and proportionality and to avoid the situation where both law enforcement and the Internet community would have to deal with a patchwork of diverse technical and legal environments.*

There are quite different important concerns to be taken into account. On one hand, data protection supervisory authorities have considered that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes. On the other hand, law enforcement authorities have stated that they consider the retention of a minimum amount of traffic data for a minimum period of time necessary to facilitate criminal investigations.

Industry has an interest to co-operate in the fight against crimes like hacking and computer-fraud, but should not be confronted with measures that are unreasonably costly. The economic impact of any measures should be carefully analysed and compared with the effectiveness of such a measure in the fight against cybercrime in order to avoid making the Internet more costly and less affordable for users. Adequate security of any retained traffic data would have to be ensured.

In any case, industry will have a key role to play in contributing, to the process of creating a safer Information Society. Users should have confidence in the safety of the Information Society and feel protected from crime and from infringements of their privacy.

The Commission fully supports and encourages a constructive dialogue between law enforcement, industry, data protection authorities and consumer organisations as well as other parties that might be concerned. Within the framework of the proposed EU Forum (see point 6.4 of this Communication), the Commission will urge all the parties concerned to discuss in-depth, as a matter of priority, the complex issue of retention of traffic data with a view to jointly finding appropriate, balanced and proportionate solutions fully respecting the fundamental rights to privacy and data protection. On the basis of the outcome of this work, the Commission will be able to assess the need for any legislative or non-legislative actions at EU level

3. QUESTIONS

Questions to industry:

1. **What data are currently retained by industry and for what purposes?**
   - *What are the criteria that determine how long they are retained?*
2. **Is it necessary to retain data for network security and/or fraud prevention purposes?**
   - *Why? What data need to be retained and for how long?*
   - *What is meant by network security? What is meant by fraud prevention?*
   - *Are there any other purposes which would require such retention?*
3. **What is the relative importance of each type of data?**
   - *What storage methods are used?*
4. **How does the service provided affect the issue of data retention?**
   - *Are there different forms of data retention practices (if any) depending upon the business model?*

   - *How does the billing method affect the issue of data retention?*

5. **What are the kind of data most often required by law enforcement?**
   - *What data are less frequently required?*
   - *Under the current practices have you been able to provide the data in these cases?*
   - *What is the cost of a law enforcement request?*
6. **How do you expect future developments to affect the issue of data retention? (**Examples include new services, real time automated processes, convergence, increasing bandwidth and increasing prevalence of flat rates)
   - *Do/will technological developments allow a computer-literate criminal to operate in a manner that is technically untraceable?*
7. **What are the financial implications of obligatory or voluntary retention?**
   - *What efforts should be made to address these implications?*
8. **What are the costs associated with data retention?**
   - *In which part of the process are most costs generated?*
   - *Is it in storage, retrieval, processing, acquiring the necessary equipment to perform those functions, in the internal business structure?*
   - *What are the costs related with making the available data admissible evidence before a court of law?*
9. **Do the current diverging approaches in Member States on the issue of data retention pose serious problems to industry?**
10. **Are there any other industry interests that need to be taken into account?**

Questions to law enforcement:

1. **In what concrete cases do law enforcement authorities get traffic data from electronic communications services providers?**
   - *What are the conditions (legal or other) to get them?*
   - *Do the conditions limit access to traffic data only belonging to suspected persons, or can other persons have their traffic data disclosed for the purpose of a criminal investigation?*
   - *Which measures are taken in relationship with regulated professions?*
2. **How do law enforcement authorities usually use that data?**
   - *Are they used as intelligence or are they used in court as admissible evidence?*
   - *How is content data excluded?*
3. **What are the traffic data most commonly requested during investigations?**
   - *What traffic data are usually available under the current practises and how useful have they been in police investigations?*
   - *Has there been demonstrated need for more than what is currently accessible, or you think that the current situation could be maintained?*
   - What is the response time law enforcement expects from the service providers?
4. **Have there been cases where absence of data has led to failure to investigate?**
   - *Are there any statistics available on unsolved crimes, due to lack of electronic evidence?*
   - *How often is traffic data used as admissible court evidence?*

5. **Are there evidential and procedural problems associated with requests for data, particularly in relation to their acquisition and use?**

6. **Is it necessary to retain traffic data of all users of electronic communications for the prevention, investigation, detection and prosecution of criminal offences and if yes, why?**
   - *Can you illustrate this necessity by using concrete examples?*
7. **What data would need to be retained by electronic communication operators and for how long?**
   - *What is the relative importance of each type of data?*
   - *How long does it take in the course of an investigation to determine whether there is a need or not to acquire traffic data*
   - *What kind of electronic communications are in particular relevant?*
   - *What is the relevance of each type of traffic data in relation to the concrete crime?*
8. **Are there any cross-border requests to acquire traffic data?**
   - *How often do law enforcement authorities need traffic data from service providers established in another Member State?*
   - *Do they get it? If not why?*
9. **Are there any other means at the disposal of law enforcement authorities to identify a suspect using an electronic communications network?**
10. **Does data processed by industry on a voluntary basis within the context of the data protection legislation meet the concerns of law enforcement regarding data retention?**
11. **Are reports on the use of traffic data in the framework of crime policy published in your country?**

Questions to data protection authorities, civil liberties and consumer organisations:

1. **Why traffic data should be erased after completion of a communication for data protection and privacy reasons?**
   - *Are traffic data sensitive and why?*
   - *Are there traffic data with different degrees of sensitivity?*
   - *Is there a special problem related to location data ?*
2. **What is the relation or similarity between retention of traffic data and interception, if any, from a data protection perspective?**
3. **Why does mandatory retention pose legal problems with regard the European Convention for Human Rights?**
   - *To what extent does it depend on the amount and type of data or the duration of the retention?*
   - *Why does the state has the burden of proof on the necessity to retain traffic data?*
   - *Why does the retention of traffic data of all users of electronic communications services without the condition of concrete suspicion on each individual cause problems?*
4. **Are data protection authorities aware currently of any data retention practice within their jurisdiction?**
   - *Do data protection authorities have a supervisory role in data retention and access practices by LEA within their jurisdiction?*

5. **Would mandatory transfer of the necessary data to a trusted third party infringe personal data protection ?**
    - *Which entities could fulfil such a role ?*
    - *What conditions should apply for storage of data by third parties ?*
    - *What conditions should apply for access to data stored by third parties ?*
6. **What are the views of the consumers on the issue of data retention?**

Questions to all:

1. **What other questions than those mentioned already in this working paper would need to be addressed in your view?**
2. **Given the need to limit to the absolute necessary the amount of data that could be retained, do we need to define the relevant data not as "traffic data" but in a different way and possibly use a different term, such as for instance "connection data"?**
3. **What is the regulatory situation and the plans for traffic data retention in your country?**
    - *What elements merit particular attention?*
    - *Why is traffic data retention considered necessary in your country?*
    - *Why are other means of law enforcement authorities to investigate crime are considered not sufficient?*
4. **Additional remarks?**

ANNEXES

Annex I: Business and technology-related issues

1.1 Types of data

Different network applications and services use and generate different types of data, data which is used for certain specific purposes, data which may or may not be stored for later use or analysis, which may or may not be transmitted to another party.

On the telephone network there has been an obvious distinction between content data (a conversation) and billing data. Prior to the introduction of digital switches and the possibility of itemised billing, billing data simply consisted of the number of pulses recorded. Itemised billing means that more information is recorded (and presented to the consumer), if only for the more expensive calls. Itemised billing does not normally cover local calls.

Telephone companies have therefore in the main collected data to ensure that their customers pay the correct amount for the services used and that people cannot dishonestly use the services for free. To perhaps state the obvious no telephone operator feels it is necessary to record conversations as part of their normal business, but they try to run secure billing systems.

Mobile telephony, and the possibility of roaming, in conjunction with the business models adopted means that more data is collected. A single call between two users who are each roaming away from their home networks can involve data from four networks. In addition given the price of the services involved fraud or disputed payment is a problem and therefore location data is also recorded. More services are being added to basic voice telephony: SMS, iMode, WAP, etc.. With the move to 3G mobile the amount of new forms of data potentially available to operators will dramatically increase, and perhaps then be used by them in delivering new services. With SMS the content of communications could now be stored by the service provider for a period of time.

In addition to the data which is more or less obvious to a mobile user and may appear in their bill – the telephone numbers used, times and durations of calls and networks/location – there are several other data items. In GSM handsets the mobile equipment itself is identified IMEI (International Mobile Equipment Identity) Number. The SIM card is similarly identified by an IMSI (International Mobile Subscriber Identity). Calls involve encryption keys and random numbers used to secure the conversation.

With the Internet many things change. For example the separation between content and the equivalent of signalling data is at the very least blurred: the equivalent of some signalling information is contained within the header of IP datagrams; the headers of e-mail messages are used to store information by intermediaries; URLs are often given as easy substitutes for content (sending a pointer to some data rather than the data itself). In addition the variety of services and the variety of systems involved means that information about a particular activity may be scattered. A user may or may not decide to use the e-mail service of their ISP: they may use a service provided by a third party. Users may implement applications and use tools (from games to encryption programmes) without needing to inform the network that provides access to the Internet. An indication of some of the diversity of data involved in the Internet can be found in the annex to this note.

The kinds and amounts of data that often needs to be gathered is in some cases determined by the business model. Even within telephony there is a variety of levels of detail: ranging from the case of a fixed telephone at particular premises where the bill is by direct debit through to pre-paid mobile phones where scratch cards are used. An ISP which allows dial-up access and charges for connect time will obviously need data which different to one which offers a flat-rate ADSL connection.

Efforts have been made in the area of legal interception to define International User Requirements (IUR) 1996 (OJ C 329, 4-11-1996, p.2) which detail the general operational needs on interception and/or data searches in relation to enquiries. The IUR relates these operational needs with respect to public telecommunication networks and services. The data involved obviously goes beyond what could be considered appropriate for data retention and obviously goes significantly beyond what any network operator or service provider would need. The requirements though do present a sort of super check-list of the sort of things LEA are interested in.

What is then meant by traffic data, the data thought to be concerned when data retention is often discussed? Is there any consensus on what is involved? Would another term be more appropriate?

1.2 The technology perspective

The telephone system provides effectively a single service: a channel for voice communication. The bandwidth is low and, for some time now, the signaling data has been kept effectively separate from the voice data. Telephone conversations have beginnings and ends. They normally take place between two individuals.

Modern broadband connections are multi-service and multi-user. An individual can be doing several things at the same time over the same connection: looking at several web-sites; listening to the radio; sending e-mail; uploading a file, etc.. These different activities will involve quite different and quite independent service providers. The same connection can be used at the same time by different people in a household or in an office. Some of these activities are not “closed”: when does somebody actually stop looking at a particular web-site?

Certain tendencies are clear. Bandwidth to the home and to the office will continue to get cheaper. The number and variety of services will increase. Distance learning is common-place. Already people are having medical examinations over networks and the first medical procedures have been carried out. The number of mobile and wireless terminals will increase. The number of different access models will increase, including those which provide anonymous access such as cyber-cafés or wireless lans in public spaces (including neighbourhood networks). Finally the number of devices connected to the network will increase. Much of the future traffic on the Internet will not be people communicating but devices communicating: the micro-wave, the fridge, the car, the vending machine.

In this sort of environment encryption either of the contents of communication (of an e-mail or a web-session), or for authentication or to create virtual private networks will become commonplace.

These tendencies have general implications for data retention. Given the mass of data the data useful to retain could become increasing difficult to identify and the potential amounts increasingly difficult to store and even then interpret.

1.3 Network security and current practises

Industry has legal obligations, contractual requirements and commercial incentives to secure data, particularly when it is personal data, and services. Industry also needs to operate its services efficiently which naturally involves a degree of monitoring, historical or otherwise. How the security objectives in particular are met and can be met depends in part on the type of service and the particular business model. It also depends on the realistic threats that can be envisaged and the responsibilities that can be assumed.

Network security systems analyse the network traffic and log certain types of data, based upon which the system administrators can manage and protect their networks. Network security in this sense should be seen from the perspective of actual threats against the integrity, proper function and availability of the network, such as denial of service attacks or large scale spamming, and not illegal acts of any kind that could be committed or facilitated through the use of the network. Network security in this perspective is seen to be separate from the security required by a network user whether individual or corporate. They in turn will have their access control systems and firewalls. Each actor then has different security requirements and indeed these requirements may vary markedly even within different parts of the same information system, with for example more stringent controls and logging for updating information compared with simple browsing of the same information.

Certain types of data are useful from a historical perspective, in order to understand events and the performance of the network.. They are also necessary in the actual day-to-day secure management of the network. Network and information security has become an increasing concern for industry, due to market and regulatory developments. Data protection legislation in Europe obliges service providers to safeguard the security of services provided and to maintain and to process the personal data under their control in a secure manner.

What is not clear is the understanding of network security and the extent to which data tends to be logged in practise, either in terms of the kinds of data and the time-scales. In particular it is not clear to what extent companies have formal policies on for example how long data should be kept or if it is simply a case that logs are overwritten in line with storage management requirements.

1.4 Business models and cost attribution

Some business models depend on much more being known about the users, including details of what they are doing on the network. A telephone company offers different tariffs for calls to different people, for calls at different times of the day and for calls to different countries: for international calls each is billed separately. A typical ISP on the other hand does not charge for individual e-mails and makes no distinction by destination. Neither do they charge differently if the user is browsing a site which is local or on the other side of the world. ISPs who operate a service based on dial-up access and a fixed amount for a fixed number of hours obviously need to record when a user logs in and logs off in order to be able to bill that user. ISPs who offer an always-on flat-rate service may record quite different data.

As the different models involve quite different types of data and quite different volumes of data any discussion of mandatory data retention becomes problematic, even if financial compensation or cost recovery were involved. The costs of retaining certain data items under certain models could be fairly low; the same data under different models could be quite high. On the other hand fixing business models or limiting innovation also presents obvious problems.

It is also of course difficult to ascertain the value of the data retained from the LEA perspective. The issue of overall resource allocation in the fight against crime is a very difficult one and not one that can be dealt with here. But the need and value of the data, the sort of crimes it would help solve, their frequency and severity, somehow needs to be considered if cost attribution question is to be tackled.

Annex II: Internet Data Types

One source identifies over 700 “well known” Internet services that are provided by various service providers in different geographic locations. Examples of the most common services and the most common types of data are listed below:

This sample gives just a flavour of the richness of data types involved in the Internet environment: it is by no means complete. The different elements are used and stored in different places. The level of trustworthiness of the data also varies widely, especially if it is used for purposes for which it was not collected.

- PCs
  - copies of e-mails sent and received
  - book-marks
  - history of web-sites visited
  - cookies accepted and refused
  - cache copies of web-data
  - user IDs and passwords

- Network Access Systems (NAS) (dial up services)
  - Access logs specific to authentication and authorization servers, such as TACACS+ or RADIUS used to control access to IP routers or network access servers
  - Date and time of connection of client to server
  - User ID
  - Assigned IP address
  - NAS IP address
  - Number of bytes transmitted and received
  - Caller line identification

- Email servers

  - SMTP log
  - Date and time of connection of client to server
  - IP address of sending computer
  - Message ID
  - Sender e-mail address
  - Receiver e-mail address
  - Status indicator
  - POP log or IMAP log
  - Date and time of connection of client to server
  - IP address of client connected to server
  - User ID
  - In some cases identifying information of e-mail retrieved
  - File upload and download servers

- FTP log
  - Date and time of connection of client to server
  - IP source address
  - User ID

  - Path and filename of data object uploaded or downloaded

- Web Servers
  - HTTP log
  - Date and time of connection of client to server
  - IP source address
  - Operation (types of command)
  - Path of the operation
  - Last visited page
  - Response codes

- Usenet
  - NNTP log
  - Date and time of connection of client to server
  - Protocol process ID
  - Host name
  - Basic client activity (but not the content)
  - Posted message ID

- Internet Relay Chat
  - IRC log
  - Date and time of connection of client to server
  - Duration of session
  - Nickname used during IRC connection
  - Hostname and/or IP address

ANNEX III: Relevant Documents

- *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Communication of the European Commission, 26 January 2001, COM(2000)890, http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm
- *Network and Information Security: Proposal for a European Policy Approach*, Communication of the European Commission, 6 June 2001, COM(2001)298, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm
- JHA Council conclusions: http://europa.eu.int/comm/justice_home/news/terrorism/index_en.htm
- *Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes*, 7 September 1999, Art. 29 Data Protection Working Party, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_99.htm
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L24/1 of 30.1.98, http://europa.eu.int/ISPO/infosoc/telecompolicy/en/harmony.htm
- Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, European Commission, 12 July 2000, COM(2000)385, http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#dp
- Relevant provision of international law on privacy: European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, http://europa.eu.int/comm/internal_market/en/dataprot/law/fechr.htm
- Position de l'AFA, de l'AFORM et de l'AFORST sur le projet de loi Sécurité QuotidienneI, 10 octobre 2001
- Charter of Fundamental Rights of European Union , Articles 8 and 9, http://europa.eu.int/comm/justice_home/unit/charte/index_en.html

******