



Brussels, 04/04/2007
JLS D1/NK/D (2007) 4654

SUMMARY REPORT
MEETING ON IMPLEMENTATION ISSUES SURROUNDING THE DATA RETENTION
DIRECTIVE (DIRECTIVE 2006/24/EC) OF 14 MARCH 2007

The meeting was attended by some 170 participants made up of representatives of Member State authorities, the European Parliament, Data Protection Authorities, the European Data Protection Supervisor, the electronic communications industry and the European Commission. The aim of the meeting was to identify issues surrounding the transposition of Directive 2006/24/EC ("the Data Retention Directive").

1. OPENING REMARKS

Mme. Denise Sorasio, Director Internal Security and Criminal Justice, Directorate General Justice, Freedom and Security, European Commission opened the meeting. She noted the importance of the meeting in that it was meant to identify problems and difficulties in the implementation of the Directive, and not to discuss the merits or otherwise of data retention. She explained that there will be further meetings to address possible solutions to problem areas identified at this meeting.

The Directive was adopted quickly as a response to the Madrid and London terrorist attacks but is also of value regarding other types of serious crime such as child pornography. The interference caused by the Directive to the protection of personal data, is believed to be proportionate and necessary in order to achieve internal security.

The objective of the Directive is not just to retain the data but to permit law enforcement authorities to access and use such data. Accordingly it is not sufficient for industry simply to store relevant data – they must also be capable of identifying and quickly retrieving data on request of competent authorities. Although not expressly addressed by the Directive, cost reimbursement remains an important issue and one where the appropriate balance of assisting industry to implement effective retention and retrieval systems and avoiding unlawful aid must be carefully addressed.

The EU should create a Data Retention Platform whose members would be drawn from experts from the participating stakeholder groups with the aim of resolving difficulties in implementation of the Directive and the exchange of best practice.

2. DATA PROTECTION AND PRIVACY ISSUES

2.1. Mr. Jim Gamble – Chief Executive, Child Exploitation and Online Protection Centre, UK

Mr. Gamble considered the Directive an opportunity for cooperation to make life more secure. The national authorities should not focus merely on using the Directive to fight terrorism but also to combat other types of crime. It is very important for law enforcement authorities to have access to data when they need them. Data can be used in order to understand the reasons for which a particular crime has been committed by looking at historical data, e.g. why the London bombings happened, who the terrorists were, with whom they associated.

Mr. Gamble stressed the importance of cooperation between law enforcement authorities and industry and that reasonable and appropriate compensation of the costs incurred by industry in providing access to data is important. Law enforcement authorities should try to access data only when necessary in order to minimise the costs to industry. He noted that he would like to have the longest possible period of retention of data, because the data that relate to the planning of a crime is usually older than 1 year.

2.2. Mr. Hielke Hijmans, legal advisor to the European Data Protection Supervisor

The EDPS and the Art.29 working party have been critical of the Data Retention Directive. But since this was already enacted, one had to examine the ways to implement it. The Directive has important consequences for society, citizens, for private companies and for law enforcement authorities. Data protection is a fundamental right and normally data must be erased when no longer needed. The Directive goes against this tradition and makes it obligatory to retain data even though no longer needed.

The Directive should apply only to communications and not to the content of these communications. It was hoped that Member States implement the Directive in this manner. He criticised the D. as being full of exceptions, even though the purpose was to harmonise - for example costs, periods of retention, types of data and access have not been harmonised. Mr. Hijmans noted that the implementation of the Directive should be guided by necessity and proportionality and referred to the principles on implementation issued by the Article 29 working party.

3. REIMBURSEMENT OF COSTS; LIABILITY OF SERVICE PROVIDERS AND OTHERS

3.1. Mr. Hakan Hjelmestam, Information Risk Manager, TeliaSonera

The fight against crime is a task for society which should therefore be responsible for the costs. If the private sector is forced to bear these costs this will be a form of hidden taxation. From a market perspective, an arms length distance should be ensured between commercial activities and data retention obligations. Service providers otherwise run the risk of having their image and brand associated with law enforcement, thereby negatively influencing their customers and the roll out of new services.

The approaches taken in three Nordic countries to cost reimbursement are:

- Finland: cost reimbursement for both investment and operations
- Denmark: Authorities reimburse for each individual order/request

- Sweden: Still ongoing discussion, no suggestion yet.

Norway, though not an EU member state, is also working on a national instrument.

3.2. Mr. Simon Persoff- UK Internet Service Providers Association

Industry appreciates that it can play a role in assisting law enforcement in investigating terrorism and serious crime. Indeed, it has already proven to be a very useful partner in past investigations and day to day enquiries. This is so because industry sees this collaboration not only as a legal obligation, but also as an issue of corporate social responsibility. As a consequence, the vast majority of UK industry has no problem with the concept of data retention. Government should focus on the biggest companies. In UK it should be possible to capture 95% of the data by focusing on the larger providers.

Retention of data must be addressed alongside processes for retrieval and disclosure of data, and lawful interception. The data provided by industry has to be of real use to investigators. It is important that the mechanisms of data transmission meet law enforcement requirements. This implies for Governments and law enforcement agencies to pay for the information received, as data retention is a very costly burden for companies. If law enforcement agencies and the government do not pay for the information, industry may not have enough funds to collect quality data. Cost recovery should include capital expenditure on retention, extraction and delivery mechanisms and their operation and maintenance. If government reimburses only costs which are reasonably incurred, SP considered there should be no State Aids issue.

3.3. Mr. Simon Watkin, UK Home Office

Focus should be on the data rather than the providers – there is a need to ensure that data are being retained which are likely to be of value to law enforcement effort. For this purpose the UK has developed a Code of Practice. Retention of data is relatively straightforward – more difficult is the effective retrieval of the right data. The aim is to ensure an approach which has close to zero cost for industry. In the UK, the current operating costs for retrieval and disclosure of data vary between 26 and 29 million euros per year. The capital cost for retention, retrieval and disclosure solutions is equivalent to 10 million euros per year over five years. Future operation and maintenance cost are expected to reach between 9 and 12 million euros per year. A programme is being developed for the entire UK industry, which will cost 27 million pounds. The latter will allow both the Government and industry to make important savings. Cost reimbursement has wider implications also, for example it impact on data protection issues – if authorities have to pay for retrieval and other costs, they are more likely to ensure a limited and focused approach for data requests.

3.4. Mr. Jack Wraith, Telecommunications UK Fraud Forum

The ACPO Data Communication Group is responsible for the management of the strategic relationships between the Police Service and the Communication Industry and provides the conduit whereby matters of common concern can be addressed and actioned between these two groups. It brings together all relevant branches of industry and government expertise. If the Directive is to be effectively transposed in the Member States, they will need to bring together industry and government bodies to ensure effective cooperation.

4. BENCHMARKING AND STANDARDISATION

4.1. Mr. Mario Filipponi, European Competitive Telecommunications Association: Benchmarking Report on Data Retention Implementation across Member States

The ECTA Benchmark was created for two reasons, namely to identify best practices and provide ECTA businesses with a tool to track the main cost drivers. To date this process has not been very successful. We are currently six months away from the implementation date and it has not been possible to gather significant meaningful information. Only one Member State has implemented the Directive. Very few Member States have produced advanced drafts and the position of Member states with pre-existing legislation is not clear. They are unable to share any meaningful information on how the implementation should be done. The following information is lacking:

What kind of data should be retained? / Who is going to retain the data? / For how long it is supposed to be retained? / Under which security conditions? / What is the definition of "serious crime"? / To what extent can data be centrally stored? / Who can access the data and how?

In conclusion, Mr. Filipponi said there is a pressing need for a structured dialogue on these issues between business and law enforcement to identify what is technically and economically feasible.

4.2. Mr. Peter van der Arend Chairman European Telecommunications Standards Institute Technical Committee on Lawful Interception and Mr. Mark Shepherd, ETSI Rapporteur for Retained Data Specification: ETSI Work on a Handover Specification for Retained Data

The specification work underway within ETSI does not address how data are collected but only how they are handed over and is therefore only one element of the overall data retention puzzle. A good handover interface is important both for government and industry. A common interface is quicker to implement, more reliable and cheaper. The approach consists of setting up a framework standard and of building services as they are needed. What can people do? Get involved to help shape the standard, meet interested parties and contribute to development of the standard. The aim is to have a good draft of the standard by September 2007.

5. DEFINITION OF “PROVIDERS OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES OR OF A PUBLIC COMMUNICATIONS NETWORK”

5.1. Mr. Achim Klabunde, Head of Sector DG INFSO: Definitions of key terms

The Data Retention Directive builds on several other, pre-existing legal instruments. It particular relates to the ePrivacy Directive 2002/58/EC, which is part of the regulatory framework for electronic communications, which builds on the Framework Directive 2002/21/EC. It also refers to the Data Protection Directive 95/46/EC. The definitions used in the Data Retention Directive come from the Data Retention Directive itself, the e-Privacy Directive, the Framework Directive and the Data Protection Directive.

In the Data Retention Directive itself, we can find definitions of 'data', 'user', 'telephone service', 'user ID', 'cell ID' and 'unsuccessful call attempt'. The e-Privacy Directive provides the definitions of 'user' (overridden by the Data Retention Directive), 'communication', 'traffic data' and 'location data'. The Framework Directive defines 'electronic communications network', 'electronic communications service', 'public communications network', 'provision of an electronic communications network' and 'user' (overridden). Finally, the Data Protection Directive provides definitions for 'personal data' and 'processing of personal data'.

Definition of provider: the text used in the Data Retention Directive mentions “Providers of publicly available electronic communications service or of communications networks”. The definition is set in the Framework Directive and referred to in other Directives. According to the scope of the eCommunications framework, this definition covers economic actors in electronic communications, providers of fixed telephony, mobile telephony, Internet access, Internet e- mail and internet telephony. Outside the scope are providers of Information society services, such as content services, web services (explicitly excluded from the Framework Directive) and in house communications.

5.2. Mr Sebastian Bockemühl, Federal Ministry of Justice, Germany: German draft proposal

The German draft law does not contain a specific definition of 'provider'. It will refer to providers of the services listed in Article 5 of the Data Retention Directive. Accordingly, the German law distinguishes between the provides of

- Telephony services (fixed, mobile, internet),
- E-mail services and
- Internet access services.

The current draft proposes to add a new Article 113a to the existing telecommunications law (TKG-E), imposing the obligation to retain or ensure the retention of data, and listing the data elements to be retained by service according to the service types defined above.

5.3. Mr. Simon Kang, Director Technology Standards, Compliance and Security CTO Organisation at Liberty Global Europe

There is a need to raise awareness about the technological complexity in implementing the Directive's requirements which are currently ambiguous. There is a need to have clear requirement specifications. It is also important to have standards driven technical solutions to ensure interoperability, cost efficiency and consistency across Member States.

Some issues raised by the Directive require further clarification: What is in and out of the scope? / Definition of serious crime / Required response time / Centralised or decentralised storage? / Format of LEA queries. Uncertainty around these issues has produced difficulties in business planning process.

There is a need to establish an EU managed industry working group to develop consistent solutions in these areas.

6. DEFINITION OF DATA TO BE RETAINED

6.1. Mr. Michael Bartholomew, Director European Telecommunications Network Operators' Association: Data to be retained - industry perspective

This should be the beginning of a dialogue with far reaching consequences for citizens. We have to assure that implementation is done in a balanced way. Data retention requirements should not prevent innovation from operators. The cooperation with law enforcement has to be reaffirmed. There has been little progress in the implementation process, as there is almost no information available. Only Denmark has implemented the data retention Directive.

The most important question is who will store the data and what data will be stored. This is related to the problem of duplication and involves very complicated technical operations. It is crucial to identify what is important for law enforcers and what is feasible by the operators. Industry has serious doubts about the effectiveness of the Directive. The Directive will affect providers in very different ways because of network architecture and geography. There is no universal solution. The cost of implementing the Directive is directly related to the cost of implementing new systems. Private companies should not bear the costs alone. There should be compensation. Policy makers have to take into consideration the technical limitations and industry experience. It is regrettable that there has been only limited dialogue – which means that detailed dialogue must begin now.

6.2. Mr. Luut Mol Lous, Ministry of Justice Netherlands: NL planned approach to the data to be retained issue.

There are different ways to determine the data to be retained. They can be defined through categories, definitions in law or by lower ruling, by positions of the parties concerned or by setting up a list. The Netherlands chose to insert the definition of the data to be retained in their communication law.

Model of guideline on data to be retained:

<p>1. Fixed telephony</p> <ul style="list-style-type: none">• Identification data• Location of connection to network• Date and time of start and end of communication• Bearer service <p>2. Mobile Telephony</p> <ul style="list-style-type: none">• Bearer/ teleservices• IMEI/ IMSI• Prepaid: data and time initial activation of service and location label from which service was activated• Location labels during communication• Data identifying geographic location of cells <p>3. IP Access</p> <ul style="list-style-type: none">• User ID• Identification Data• IP address• Date and time of log- in and log- off• Data to identify destination of communication in case of Calling-in, Wifi, DSL, Cable, VPN, GSM/ UMTS, GPRS

4. E- mail

- IP- address of other identification
- E- mail address sender and receiver
- E- mail address intended receivers
- Bcc addresses
- Other e- mail addresses client
- Date and time of communication
- Log in name/ user ID
- Internet Telephony
- Identification Initiator
- Identification Receiver
- Identification forwarded call
- OP- addresses of all parties
- Identification data
- Date and time of start and end communication
- Log in name/ user ID
- CIDEK (G711, MPEG4)
- Protocol (SIP, H323)
- Services with PSTN gateway)

6.3. Mr. Kurt Alavaara, Security Police Sweden: Definitions of Data to be retained according to the Swedish Proposal

The definitions of the data to be retained are still under discussion. They are yet to be approved and can still be modified. Currently there is a number of data which companies are asked to keep.

5. In the case of telephony:

- calling and called telephone number
- The number dialled or the number/s if the communication has been forwarded or transferred
- Information about the subscriber or registered user (name, address)
- Unsuccessful telephone attempts
- Date and traceable time when the communication started and finished
- Service used, information stored no matter if a communication has been established or not

6. In the case of mobile telephony:

- Calling and called parties mobile subscriber identity
- Calling and called parties equipment ID
- Date and traceable time and location label for the first activation of a pre-paid anonymous service
- Location label when communication started, finished and once every hour for ongoing communication

7. In the case of IP telephony:

- User's IP addresses
- In the case of message services (e- mail, SMS, MMS):
- Sender and receiver identity
- Information about the subscriber or registered user
- Date and traceable time for the exchange of messages and log- in, log- off to the message service
- End points, necessary to identify the users communication equipment

8. In the case of Internet services:

- User's IP addresses
- Information about the subscriber or registered user
- Type of internet access used
- End points or information about transmission (term still under discussion)

7. APPLICATION OF THE DATA RETENTION DIRECTIVE TO DATA RELATING TO INTERNET ACCESS, INTERNET TELEPHONY AND INTERNET E- MAIL

7.1. Mme. Christine Moreau, French Ministry of Justice and Mr. Christian Aghroum, Direction Centrale de la Police Judiciaire: The legal and technical aspects of the French Model

Depuis 2001, il existe une loi en France pour le besoin de conserver les données techniques de communication pour des enquêtes pénales. Il n'y a donc pas de contradiction entre la législation interne et la Directive.

Les données sont gardées pendant un an et la législation permet aux opérateurs de garder une partie des données pour leur propre utilisation. C'est le budget du Ministère de la Justice qui supporte les coûts de demandes de données aux opérateurs. L'opérateur est remboursé en fonction de l'information qui lui est demandée. Ce que les opérateurs conservent pour leur propre besoin n'est pas pris en charge par le Ministère. Il n'y a ni pertes ni bénéfices pour les opérateurs. En ce moment le Gouvernement Français est en train de recenser toutes les possibles données que les opérateurs pourront transmettre en matière de service d'Internet. Ils étudient également les frais de chaque donnée.

Il est important que les informations soient accessibles. La technologie ne facilite pas les enquêtes de police. Il est difficile de décider quelles sont les données nécessaires avant l'infraction.

7.2. Mr. Kurt Einzinger, Vice President EuroISPA

Most of the focus of discussions so far has been on telephony. For Internet service, the changes are even greater than for telephony providers. Currently, there have been no advanced implementation proposals from member states (at least in relation to Internet data) and the implementation deadline for 16 Member states is the 15th of March 2009.

Fundamental questions: Who should retain data? Is an ISP required to retain data that just passes over its network, or only at the edges? For the ISPs in the middle, it is technically very difficult to retain data and there are significant cost implications. Is it only the larger ISPs which are caught or also those with only a few hundred customers? Concerning duplication, the Danish legislation states that where data can be retained by more than one provider, it must be retained by at least one of the providers. Who has access to retained data? This question has an impact on how ISPs organise their interfaces for retrieval.

Agree with UK view that costs have broader implications and will encourage more focused LEA requests where they have to pay for retention and retrieval. ISPs shave privacy obligations towards their customers – so the question of who has access to retained data needs to be very clear. It should not be for the ISP to decide on whether to grant access so access should always be on the basis of a court order.

Practical issues for ISPs: E- mail data - there is very little information in an e-mail that can be used to verify the sender. A lot of information can be faked. There is no continuous e- mail communication, there could be many mail transfer agents involved. There is also a problem concerning the borderline with content data.

The network and SMTP Protocol provide: IP addresses from the other side, hostnames if defined, hostname given in the greeting, envelope sender address, envelope recipient addresses, SMTP response codes at the various stages, on successful transfer usually the internal queue ID at the receiver side is returned with the final 250 ok. This is essential for tracking messages over many hops.

The message header provides: from, to, cc, subject, message ID, date, return path and received headers to track the route the e- mail took. The bad thing about message headers is that every single byte can be faked and they are unreliable if not provided by trusted hosts. None of these headers are needed to deliver a message. Furthermore, the information available for logging purposes and that which is finally written to the log depends on the software and its configuration.

VoIP: There are different technological solutions, there is no single standard. It has complex routing algorithms. Every VoIP technology has to be assessed and treated differently.

Conclusions: Relatively few Member states are at a stage where implementation is close or discussions are very advanced. EuroISPA remains worried about a lack of coordination between national implementations, especially on issues such as: exact type of data, type of storage, access rules and private standards. EuroISPA therefore strongly advocates a need for separate meetings to discuss important questions. Finally, EuroISPA underlines the relevance of the Commission's role in speeding up this process and the importance to keep in mind the civil liberties of citizens.

7.3. Mr. Patrik Falstrom, Internet Consultant

The Directive appears to be based on a model of the communication networks as they were 20 years ago, when there was only one monopoly provider; it does not really take into account the changes occurred since then and in particular, how the internet works today. Convergence has changed the entire model, and must be taken into account.

To use a service on the internet, users use services provided by several different providers at the same time, and they may use different access providers to access the same service. No single provider can provide the full picture of the communications.

The Swedish approach aims to take account of the layered structure of services in the internet. The service provider and the access provider shall take care of the data they can provide. The access provider knows from which endpoint an IP address was used, the service provider knows which service was used.

Approaches that expect the full information from the Internet transport provider cannot deliver, as the internet provider does not have the information about the services used.

8. CONCLUSIONS AND RECOMMENDATIONS

Mr. Bernd Langeheine, Director Electronic Communications Policy Development, Directorate General Information Society and Media

The Data Retention Directive was adopted in exceptional circumstances and in very little time. In these circumstances the solution at the time was to provide for flexibility. It is now urgent to find workable solutions to issues identified during this conference such as types of data, who is within the scope of the Directive and appropriate definitions. To take this forward we should waste no time in setting up an experts group bringing together representatives of the stakeholders at this conference. The aim should now be to use that mechanism to achieve greater consistency of approach to the issues raised by the Directive.