Taking on the Data Retention Directive
2010 Data Retention Conference
Friday 3 December
Brussels

Mr. Stefano Manservisi, Director-General, Directorate General Home Affairs of the European Commission

- This conference is the th ird conference on data re tention by the European Commission.
- After the first Conference in March 2007 an expert group was set up. This expert group functions as a platform on data retention. Guidance docum ents that are adopted by the expert group are not legally binding, but are influential.
- We need to create the right balance between security and data protection.

Mr. Paul van Thielen, Director General of the Belgium Federal Judicial Police - presidency of the Council of Ministers of the European Union

- Six countries have not ratified the Directive.
- Facebook and Second life are not included in the Directive. It could however be useful to think about including these.
- Only the comm unication from and to DSM are covered by th e Directiv e. Communication between two com puters is not covered under the Directive and criminals know this.
- This Directive should only apply to terrorism and organized crime.

Mr. Mátyás Hegyaljai, JHA Counsellor on behalf of the incoming Hungarian Presidency of the Council of Ministers of the European Union

- Emotion displaces often the rational debate with regard to data retention.
- A Hungarian human rights group filed a claim at the Hungarian Constitutional Court with regard to data retention.
- Before the Directive was in place, Hungary retained already data.

Mr. Peter Hustinx, European Data Protection Supervisor

- We have followed the creation, im plementation and evaluation of the Directive.
- We were part of the art. 29 W orking Party th at wrote a c ritical report on the Directive. We also have asked a ques tion to the European Court of Justice about the Directive.
- There are s ubstantial in terferences with the r ight to privac y. It is the most privacy invasive document ever adopted if you look at the scale and number of people affected by the Directive. Strong legal safeguards are therefore needed.
- Current EU law with regard to d ata re tention states th at it needs to be proportionate and strictly necessary. It is h ighly doubtful whether sy stematic data retention on such a large scale is 'strictly necessary'.
- There should be an obligation to evalua te the instrum ent. Concrete number and figures should assess the effectiven ess of the instrum ent. The evaluation

that is going to take place needs to show this. I am doubtful whether we will have convincing facts whether the Directive is useful.
- The Directive failed to harmonize national legislation and has lead to legal uncertainty.
- The Directive is also not limited to only serious crime. There is no definition of serious crime in the Directive. There are discrepancies between the MS with regard to the implementation. This is explicit stated in the Directive --> 'Diverging implementation laws'.
- MS still believe that they are allowed to use data retention for other reasons that are not covered by the Directive.
- The Bundesverfassungsgericht in Germany has put limits on the use of the Directive in Germany.
- Not only for the retention of data there should be safeguards, but also for the use by law enforcement agencies.
- Specific rules on access and the further use of the information should be in place. MS should not be able to use the Directive for additional purposes.

Mr. Lewis Benjamin, Deputy Chief Constable - National Coordinator on Serious Organised Crime - member ACPO

- The retention of communication data gives us vital information to do our work and solve cases.
- We have a lot of evidence in the UK that the Directive is effective
- To retain communication data can also show somebody's innocence.
- There is a collaborative working group in the UK to see what the requirements should be to retain communication data.
- The UK government funds the retention of data.
- Necessity and proportionality is absolutely necessary here.
- Criminals are getting more sophisticated. In order to be in the same pace as them we need to get more sophisticated as well.

Mr. Ilias Chantzos, Director EMEA & APJ, Symentac Corporation

We build the technologies to retain data.

<u>Expectations for the future</u>:
- Access will become mobile and device-agnostic.
- Business and personal digital personae have merged.

<u>Consequences</u>:
- Exponential growth in the amount of traffic data
- Criminal activity will increase
- A lack of information trust will exist. There will be 100 attacks per second that we will be able to stop. There will however be attacks that we will not be able to stop.

Mr. Axel Arnbak, Bits of Freedom

- Objections to this Directive have been overwhelming. The Commission takes legal action to MS that are not implementing this Directive, while constitutional courts in these MS have ruled that the Directive was not necessary.
- Indiscriminate data retention creates fundamental violation of our fundamental human rights.
- Even private parties started to use the retained data for other purposes than stated in the Directive.

Seminar on Crime with regard to the Directive

Moderator: Mr. Achim Klabunde, Head of Sector, DG INFSO, Unit B1

Mr. Alexander Alvaro, European Parliament (ALDE), Committee on Civil Liberties

This Directive is invasive without the necessary safeguards. Its initial idea to harmonize legislation has not worked out.

There is a big difference in how this Directive is being implemented in the MS:
- 2600 requests in Germany to retain data
- more than one million requests in Poland to retain data

The initial idea of the Directive was always to fight terrorism. Now it has been watered down to serious crime. The concept of serious crime is different however in the different MS, which gives questions like: is there an obligation to retain data if it is not a serious crime in the state that receives a request for data?

A catalogue approach like in the European Arrest Warrant recommended by the LIBE Committee is still the right approach as it gives legal certainty. This catalogue should include:
- On what basis the Directive can be used.
- The list of crimes the Directive can be used for. These crimes should have a minimum prison sentence of plus/minus three years.

A catalogue plus approach will avoid the tendency to broaden the serious crimes category to for example the violation of intellectual property rights.

A right balance needs to be struck between human rights and the fight against serious crime.

Mr. Francis Stoliaroff, Magistrat, Mission de négociation et de transposition des normes pénales Internationales, Direction des Affaires Criminelles ET des Grâces, Ministère de la justice (France)

- Calls into question the three years that Alexander Alvaro proposes and would like to harmonize it at one year.
- Recital 25 states that the Directive is not only for serious crimes.

Mr. Gert Wabeke, manager Lawful Interception, Royal KPN (the Netherlands), part of the expert group on data retention

There is uncertainty arising for the consumer with regard to what data is stored and what it is used for.

Questions and Remarks:

- What would you say about cyber mobbing or stalking through the telephone or internet which can lead to suicide and which is not seen as a serious crime?
- Before the Directive people that would get stalked would call the telephone operator and ask for information on who has been calling them. It feels that now with the Directive in place these petty crimes are not addressed anymore.
- There is a discussion going on at the moment in Austria whether they can still investigate the crimes through billing information that do not fall within the Directive.

Alexander Alvaro

- There are enough ways to prevent stalking without the Directive.
- In some countries the telecom providers don't store data because of billing reasons.
- Why don't we use a quick freeze which is less invasive and much more targeted directly and therefore less indiscriminate? My proposal would be to combine the retaining of data for billing reasons with a quick freeze.
- If anyone wants flat rates to be covered it will mean an extension of the Directive.
- Not any crime can be investigated by any tool. This Directive is such an invasive tool that it cannot be used for all crimes.
- Data information is not there as a public good for law enforcement agencies. That's why we have data protection laws. We cannot say that because it is anyway there we can use it.

Francis Stoliaroff

- To our opinion a 6 months period of the retention of data is not enough
- We have an obligation to identify the persons and fight crime

Henry Hirsch, Home Office, London

- The UK is on the same line as France
- A lot of information is kept for commercial purposes by telecom providers, also without the Directive. This leads to the question whether the information that is kept for serious crime can be used for commercial purposes.

Wabeke

Before the Directive, data was already stored for business reasons and this data was already used by law enforcement agencies. The difference is that there is specific information now that we have to store.

Klabunde

- A good question is whether this Directive was necessary in the first place.
- An additional benefit of the Directive is that it actually gives rules on the protection of data that is used by law enforcement agencies.

Seminar on the Period with regard to the Directive

Moderator: Mr. Jacques Verraes, DG Home A3, European Commission

Dr. Hab Andrzej Adamski, Professor, Nicolaus Copernicus University, Torun, Poland

- 10 MS have opted for a year retention period for each category of data. The Czech Republic retains the traffic and location of data for 6 to 12 months.
- Three MS have defined different retention periods for internet data (Italy, Malta and Slovakia). Ireland retains data for three years. Poland and Slovenia for two years, Latvia for 1.5 years and Hungary retains data for a year. There were some unsuccessful calls in Hungary for the retention of data for half a year.

Mr. Jan Albrecht, European Parliament (greens/EFA), Committee on Civil Liberties

- The question to be answered is which data retention period, if any, is justifiable (constitutional question) and which period is political necessary. What is necessary to lower the crime level?
- Even before data retention we had clearing rates with respect to crimes committed over the internet of over 80% in Germany.
- The Directive should only be used for the worst cases of crime
- Marketing data is stored with the consent of the consumer. The data that the Directive talks about is stored without that consent.

Luc Beirens, Head of the Federal Computer Crime Unit, Ministry of Interior, Belgium

A study in 2007 looked at all the requests for an IP address and showed that

- 15% of the cases were solved after 6 months
- 66% of the cases were solved after 1 year
- 84% of the cases were solved after a year and a half
- 97% of the cases were solved after two years

Moderator Jacques Verraes

- 60-70% of data that is requested by MS is younger than 6 months.
- We have only taken MS to court for not implementing the Directive. We have not taken MS to court for not implementing the Directive well.
- There is a correlation between the length of the data retention and the amount of crimes solved by the police.

- It is different to retain data for marketing purposes than for the purposes under the Directive. Companies have to invest in different tools to retain the data for the purposes under the Directive.
- The Commission will probably restrict the parameters of the period of data retention in the next revision of the Directive.

Seminar on the Operators with regard to the Directive

Moderator: Ms. Cecilia Verkleij, Head of Sector, DG Home A3, European Commission

Mr. Luc Beirens, Head of the Federal Computer Crime Unit, Ministry of Interior, Belgium

- It should be clearer who should retain data.
- There are rather difficult definitions in the Directive with terms that are not very exact. Examples of these terms are: normally, mainly and wholly.
- The term 'provided for remuneration' might be a problem in the definition, because it does not cover free community set up networks.
- There is an exclusion of information services. The difference between providers and services exists only legally.
- The exclusion of private networks is a problem. What about the internet at a hotel?
- There is no data retained under the internet services, with the exception of data by email.
- With regard to virtual providers the question will be who is responsible for the storing and providing of data?
- In the UK there is a proactive involvement with the companies. A full market assessment is done to see which companies need to retain data. Only companies that get a notification are obliged to retain data. Besides that, the UK funds the costs of the retention of data. In most other MS there is a general obligation to retain data without making any difference.

Remarks

- There is a need to be clearer on who is doing what and who is having what data. (Member of the Expert Group)
- The operators are left alone with regard to the obligation to retain data. There is no legal guidance. (Representative of the Greek Ministry of Justice)
- There are a lot of services that are not 'caught' by the Directive.

Speech by Commissioner Ms. Cecilia Malmström

- We need security in a way that is proportional. Data retention is a vital tool in this respect and is here to stay.
- The need for a level playing field in Europe has not gone away.
- The question is what form the Directive should take and how to avoid going past its scope?

- The usefulness of the Directive is shown by how many times retained data is requested. A survey that looked at 20 MS showed that in each MS there were 148.000 requests each year.
- Many criminal investigations would not have been resolved without data retention.
- 20 MS have implemented the Directive. However, the Directive is not implemented in the same way in different MS. Amongst others, there are differences in the costs, the period and who can retain the data.
- With regard to the costs for operators we see that the health of the telecom sectors has not been significantly affected in the MS.
- With regard to the impact on fundamental rights there are no concrete cases of abuse by law enforcement agencies.
- Data retention has provided a substantial effectiveness in fighting serious crime.

The Directive leaves room to improve however and we should:
- reflect on the purpose
- consider who is allowed to access data
- look at the costs
- look at what data to retain
- address the argument of data freeze

Report of the three panel moderators

Mr. Jacques Verraes, DG Home A3, European Commission

Questions that came up during the seminar on the purpose, period and scope of the Data Retention Directive:
- If we preserve data can we do away with data retention?
- Can we have less data retention with the same outcome?

Ms. Cecilia Verkleij, Head of Sector, DG Home A3, European Commission

On modalities with regard to the Directive:
- There was a lot of interest for the UK model of a Single Point of Contact. The question arised whether you need prior or past authorization for this.
- Further education of law enforcement agencies is needed.

On authorities with regard to the Directive:
The question who to qualify for the retention of data hangs together with other issues of the Directive, such as the type of crimes committed, and thus needs to be addressed in a larger framework.

Mr. Achim Klabunde, Head of Sector, DG INFSO, Unit B1

On crime with regard to the Directive:
- What should be the treshold of the serious crime?
- What crimes should be addressed under the Directive?

On costs with regard to the Directive:
In France they are of the opinion that criminals should pay the costs, while in the UK they are of the opinion that the state should pay these costs.

On security with regard to the Directive:

- How is the Directive put in place practically?
- Should stronger harmonization practices not be put in place?
- Civil society is of the opinion that stronger safeguards need to be put in place.

Questions and Remarks from the audience

- As we do not have any harmonization of data retention at the moment, the question is what the added value of a Data Retention Directive on a European level is. (Alexander Alvaro)
- To say that the Directive is here to stay before the evaluation is completed is a pre-empted reaction of the Commission. They need to look at the question of necessity. (Platform Committee)
- More attention should be given to the idea of retaining data only once.
- There are examples of abuses in Poland. One example is that in one year there were one million requests for data.
- The problem is with the implementation. The enforcement of the safeguards is another question. (Jan Albrecht)
- Did the crime quotas improve after the Directive?

Answers by the Commission

- The evaluation by the Commission and the report by the art.29 Working Party did not signal any specific abuse. Evidence of abuse has not been made public to us.
- The Directive is based on safeguards, which are based in turn on the Privacy Directive.
- There are safeguards in the Directive. The way the Directive is implemented is not in the hands of the Commission however.
- Discussions of this Conference will be summed up into a report.