EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A: Internal security
Unit A.3 : Police co-operation and access to information

Brussels, 14 February 2011
home.a.3(2011)295871

REPORT on the DATA RETENTION CONFERENCE: TAKING ON THE DATA RETENTION DIRECTIVE

Friday 3 December 2010, Brussels

Summary
The meeting was attended by around 140 participants, including representatives of law enforcement authorities (LEAs), telecommunication market regulators, national and European Data Protection Authorities, industry associations, academia, civil society, NGOs, the European Commission (COM) and other European Institutions. Following on from two previous meetings in March 2007 and May 2009, the aim of the conference was to bring to a close the process of evaluation of Directive 2006/24/EC (the Data Retention Directive or DRD), and begin that of its review. Subsequently, concrete proposals to amend the directive will be prepared by the COM, Commissioner Malmström announced in the closing session of the conference.

During the evaluation process, nine issues were identified by the COM for discussion at this conference:

1) Purpose of data retention
2) Scope of the directive
3) Data retention period
4) Definition of serious crime
5) Authorities with access
6) Mode of access and cross-border transfer
7) Operators under retention obligations
8) Cost recovery
9) Data security

These issues were discussed in three separate seminar groups, each of which held three discussion sessions.

In annex:
- List of abbreviations used
- Conference Discussion Paper prepared by DG HOME

Plenary session

Keynote speech by Mr. Stefano MANSERVISI, Director General of Directorate General (DG)

Home Affairs of the European Commission

Mr Manservisi welcomed all participants to this, the third conference on the DRD. Highlighting the huge advances of recent years in the development of mobile telecommunications, and the growing importance of the internet, he said that society must be aware that alongside their use for business and entertainment, these technologies are also being used to commit serious crimes. A stronger alliance is needed between the private sector generating data from these technologies, and the LEAs using it to investigate crime, he emphasised.
The first conference on the DRD in March 2007 concluded that it was urgent to find workable solutions for issues on which the DRD remained inconclusive. Subsequently, the COM set up an expert group, the Platform on Electronic Data Retention, to provide guidance on the most important issues surrounding the implementation of the Data Retention Directive; the opinions of the expert group are laid down in so-called position papers. The second conference, held in May 2009, began the process of evaluation of the directive; the COM is required under Article 14 DRD to present to the Parliament and Council an evaluation of the application of the directive and its impact on economic operators and consumers. Questionnaires were sent to all stakeholder groups: law enforcement authorities, and telecommunication market regulators, the European Parliament, civil society and privacy advocacy groups, telecommunication, network and internet operators, and data protection authorities. Bilateral meetings were held with all Member States (MS). Replies to the questionnaire as well as the position papers adopted by the expert group in 2009 and 2010 have been published on the website of the conference: http://www.dataretention2010.net-/home.jsp

The work of the expert group is to assist the Commission with the evaluation of the DRD and to advise it on issues regarding the application of the Directive that provide guidance for law enforcement (what to expect) as well as latter for the private sector (what to do) and contribute to better understand the directive. The guidance documents adopted by the group are non-binding authoritative statements. The group has addressed questions such as:

1) How does the directive apply to email?
2) Should service providers retain data related to spam email?
3) What does the expression 'internet telephony'**,** as used in the Directive, mean?
4) Which law applies to data stored in a MS other than that in which it was generated?

The participation of civil society and industry in the evaluation of the DRD is crucial. The contributions made to the conference, as much as the evaluation process in itself, are vital to the future of data retention in Europe, in terms of creating the right balance between security and data protection.

Keynote address by Mr. Paul VAN THIELEN, Director General of the Belgian Federal Judicial Police – presidency of the Council of Ministers of the European Union

Mr. Van Thielen welcomed participants on behalf of the Belgian Presidency. He highlighted the importance of evaluating the directive, and the challenge faced by politicians in finding a balance between sometimes contradictory interests; protecting society, democratic values and the values of the EU. Six MS have still not transposed this directive into national legislation, he pointed out.
The rapid evolution in the mindset and behaviour of technology users should be considered. Traffic data related to technologies such as Facebook and Second Life should be covered by the Directive, as it may provide meaningful leads in criminal investigations.

Internet telephony is covered, but while traffic data from mobile phones is recorded, voice communications via the internet are not – criminals take advantage of this situation. Traffic and location data registered by service providers can direct criminal investigations; can back up an alibi

or show associations between criminals – but the criminal world is invariably looking for means of communications which are difficult to trace. In order to fight cyber crime, data needs to be kept for longer periods. The minimum retention period of six months set out in the Directive is not enough for LEAs.

Organised crime is international, and Internet Service Providers (ISPs) are usually active in several Member States (MS), so the directive should be evaluated from an international perspective. In which country and according to which legislation should data be kept, and which authority in which country should authorise access?

A balance can be found between privacy and security using stricter procedures regarding access to and use of data. Access should not be given for trivial matters, but only to fight organised crime and terrorism. Data protection should be enforced; access logs should be generated and kept.

Keynote address by Mr. Mátyás HEGYALJAI, JHA Counsellor on behalf of the incoming Hungarian Presidency of the Council of Ministers of the European Union

Mr Hegyaljai emphasised that the DRD has been the subject of considerable controversy. It is a good example of the clash between the imperatives of delivering public security and ensuring citizens' rights to privacy. The ruling by the German Constitutional Court of 2 March 2010 was emphatic that a balance must be struck between these two imperatives. Hungary has now implemented all the provisions of the DRD, but the Hungarian Civil Liberties Union has filed a motion with the Hungarian Constitutional Court requesting the annulment of the national law transposing the DRD. The Court has not yet made a decision. The incoming Hungarian Presidency believes that enabling LEAs to access communications data retained by operators constitutes a necessary and effective tool in the fight against serious crime. However, it can be difficult for MS to provide statistics to the COM on the use of telecommunications data for law enforcement purposes since such data is often classified. Mr Hegyajali hoped the COM would present its evaluation report during the Hungarian Presidency.

Data Protection Community: Presentation by Mr. Peter HUSTINX, European Data Protection Supervisor (EDPS)

Mr. Hustinx explained that the EDPS has been involved with the directive since 2005, first as an advisor to the legislator, and subsequently through involvement in the expert group and Article 29 Working Party. EDPS also intervened in the case that was brought by Ireland that went before the European Court of Justice on the legal basis of this instrument. Mr. Hustinx said that the DRD was the "most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects". He said that such a massive invasion of privacy, which allows for the retention of data on all persons in the EU whenever they use the internet or phone, needs profound justification. Current European law including the Charter of Fundamental Rights, which is now binding, requires the retention of such data to be proportionate and strictly necessary for the purposes envisaged. "Strictly necessary" means that the purposes of the measure can only be reached by applying this specific measure; if the same results can be achieved using less intrusive means, it is not strictly necessary. He urged the Commission to use the evaluation to prove the necessity of the Directive, and called it the "the moment of truth" for the instrument.

One alternative could be a more targeted approach. The evaluation is an opportune moment to show evidence in support of the claim that the DRD is a necessary and proportionate measure, and move away from the currently held "assumption" that such is the case. Without such evidence, the directive should be withdrawn or replaced by a more targeted and less intrusive instrument, such as quick freeze, which does meet the requirements of necessity and proportionality. Information

published by the European Commission has shown that many MS have been unable to provide sufficient evidence in time for the September 15 deadline for the COM to submit its evaluation of the directive to the European Council and Parliament, Mr. Hustinx noted.

The directive has failed to harmonise national legislation, which has led to legal uncertainty for citizens and operators. Moreover, the use of retained data is not strictly limited to the combating of serious crime and terrorism as the directive states it should be. The Article 29 working party said in its report last summer that there are "significant discrepancies" between MS in their implementation of the directive. This is a result of weaknesses in the DRD, Mr Hustinx believed: the wide choice of retention period, the use of undefined notions like 'serious crime' and 'competent national authorities', and the absence of rules on recovery of costs. Mr. Hustinx also said there is a loophole in the legal framework. The DRD derogates from the obligation in the directive 2002/58/EC, the E-Privacy Directive, to delete traffic data when it is no longer needed for the commercial purpose it was collected for. Under Article 15 of the E-Privacy Directive, MS can derogate from this obligation for law enforcement purposes – the objective of the DRD was to harmonise use of this derogation. However, the Article 29 Working Party found that in practise, many MS believe they are still free under the E-privacy Directive to put in place retention obligations for other reasons not covered the by data retention directive, such as for prevention and for non-serious crime. This situation undermines the very purpose of the Directive, namely to create a level playing field for business based on an equal and effective level of protection of citizens.
The invasion of privacy should be offset by a clear scope, unequivocal definitions, precise rights and obligations for MS' "competent authorities", and an equivalent high level of protection that should not depend on the intervention of a constitutional court. The Directive "only tells half the story" as it does not contain rules on access and further use of data by law enforcement. These should be included in any new or amended instrument proposed by the Commission, and not leave any room for MS to use the data for additional purposes.

Law enforcement community: Mr Lewis BENJAMIN, Deputy Chief Constable – National Coordinator on Serious Organised Crime – member ACPO

Mr. Benjamin emphasised the importance of partnership work between the communications industry, governments and LEAs both within and outside the EU, in order to detect, prevent and tackle serious crime.
Experience in the UK has shown that historic communications data is absolutely critical in the fight against serious crime, he said. Retained communications data has frequently given investigators vital information. Many serious crimes are solved not by forensics but by communications data. Criminals are forensically aware; they don't go near their victims, or crimes are committed in cyberspace. Communications data can corroborate the testimony of a witness, or can tell police how and where a victim died, and who they were with. Communications data can be particularly useful in murder investigations; Mr. Benjamin cited the case of a man who was murdered by seven Hells' Angels while driving on a motorway in the UK – all seven were convicted for life using communications data, since there were no witnesses, forensics, or confessions. Importantly, communications data can also indicate someone's innocence.

The directive provides a legal basis for retaining data which would otherwise be erased if the service provider no longer needed it. Competing interests between protecting the public and protecting individuals' data can be resolved via safeguards requiring the lawful acquisition and secure protection of that data and its deletion after the expiration of the retention period. Service providers also need help with the practicalities of the retention and retrieval of data; the UK has set up a collaborative working group on this. The directive does not contain an explicit provision on the reimbursement of costs for providers.

In the UK, the government, police and security services contribute to these costs in as far as service providers are required to do something other than their own business would require; this practise should continue. Mr Benjamin also highlighted the effectiveness of the UK's of a Specialist Communications Investigators scheme. These investigators are jointly trained by police and industry, and credited by the government to use specific law enforcement competences for the acquisition of data. It is necessary for police forces to continue updating their investigation skills, he highlighted, in order to keep abreast of modern technology, and of the increasingly sophisticated methods of criminals.

Economic Operators: Mr Ilias CHANTZOS, Director Government Relations EMEA & APJ, Symantec Corporation

Mr. Chantzos, Director of Government Relations for, *i.a*., the EU branch of Symantec, a company which offers technological tools to secure the storage and processing of large amounts of data in systems management solutions - began by asking: where is technology going and what problems does this create in terms of the DRD? He explained that users are more and more mobile and that access will become 'device agnostic' – meaning that users do not mind which device they use, rather it is connectivity (connection to the internet) that is most important. If 'device agnosticism' takes over, the problem in terms of the DRD will be increasingly the identification of *who* is using the device and their rights to content or services, rather than the question of which device individuals are using.
The trend is that people require simple and secure access to networks and information. Both for business and private use, managing data needs to be scalable and cost-effective.

Key technologies to corroborate this trend will include:
'De-duplication': the central storage of information (such as emails) which currently exists in many environments
Virtualisation: the use of multiple computers within the same machine.
Increasing use of Internet Protocol (IP) based networks
Focus on data analysis and retrieval, due to the amount of data being generated

These technologies will require:
Identity security: the ability to prove *who* accessed data, *where*, and *why*
Device security: the ability to protect machines and networks in particular by using very strong encryption
Context and relevance: ease with which data can be found, stored and retrieved
Access to the cloud (network) as an infrastructure to provide this connectivity

The consequences of these advances will be:
Shift from the current technology paradigm, which is system-centric, to an information-centric approach. The location of information – not who has it - will become most important.
Dependence on network connectivity will become key for data retention, for example the ability to run software.
An exponential growth in the amount of data generated.
Offline criminal activity will increasingly move online.
Counter-intelligence will make use of encryption technologies to prevent tracking.

The operational risks involved in these trends and required technologies are:
There will be an increased amount of security breaches
There will be a risk of a lack of availability of information
There will be new regulations on security requirements
There will be a huge information growth, both in structured form (databases) and unstructured

(communications)
The cost of managing the storage of personal information will increase
There will be information trust issues: can we trust an infrastructure which is constantly under attack, estimated at 100/second that should be stopped? In 2009 3000 new computer viruses were detected.

The challenge from an operational standpoint in terms of the DRD is to increase efficiency and reduce complexity: to better manage data, reduce the volume of data stored to cut the cost of storage, to control the data, to establish what needs storing and for how long, and to enable quick search and retrieval, and also deny access to information in justified cases.

Other issues to consider are: how to protect against information breaches, how to apply retention policies, how should information should be destroyed and when, how to link encrypted traffic data back to a person, how to address the costs involved, and instances where data in a network may be outside jurisdictional control (e.g. stored in the cloud outside of the EU).

These questions were asked when the directive was first discussed but the technology shift of the last few years calls for their re-consideration.

Civil society (fundamental rights): Mr Axel ARNBAK, Bits of Freedom

The Dutch organisation Bits of Freedom is a member of the European Digital Rights Initiative, an NGO bringing together 29 civil rights organisations in 19 MS. Mr. Arnbak said that the objections to this directive from national constitutional courts are overwhelming. He expressed his belief that in a democratic society, it is dangerous for the COM to take legal action to force adoption of that legislation. Three weeks ago, the European Court of Justice (ECJ) confirmed in the *Schecke*-Cases 92/09 and 93/09 that derogations and limitations in relation to the protection of personal data must apply only as far as "strictly necessary". This criterion requires the application of a strong proportionality test, not the concept of usefulness of data. Mr. Arnbak said he was disturbed that in a letter sent to MS on 27 July, the COM asked for data on whether the DRD was "useful".

Information technology is spreading into every part of our lives as a positive force for fundamental freedoms, business and democracy, but with the DRD in place it facilitates unprecedented surveillance of citizens, Mr. Arnbak stated that this was underestimated by the legislator in 2005. In 2010 the average European has his traffic and location data logged in a telecommunications database once every six minutes, i.e. 225 times per day. Such indiscriminate retention of data without concrete suspicion is a fundamental violation of our freedoms, Mr. Arnbak believed. Data retention is destroying our "digital ecosystems", just as fishing with dynamite destroys the marine ecosystem. For example, in a poll of 1,000 Germans from May 2008, the majority said that they would refrain from contacting marital crisis lines, drug counsellors or psychotherapists via phone or email because of the DRD. There is also a risk that retained data will be used for goals other than those specified in the DRD and even by private parties in copyright infringements. Another example is the European Federation of Journalists' (EFJ) opposition to the DRD: the EFJ believes it will damage the freedom of the press.
Mr. Arnbak cited a recent case in which a Dutch journalist (Dick Kivits) was prosecuted for exposing security weaknesses in the email account of the Dutch defence secretary; at trial he found his entire telecoms history, including anonymous sources for unrelated articles, in his file. He was not convicted but says he now feels intimidated to write further articles.

Bits of Freedom believes that the principle of indiscriminate data retention erodes the very essence of the Charter of Fundamental Freedoms. Mr. Arnbak called on the COM to reject the principle of data retention. If the COM believes in evidence-based decision-making and free and open societies,

it cannot retain the principle of blanket data retention, he concluded.

Panel discussions

The panels discussed the nine topics that the Commission had outlined in the Discussion Paper (see annex) that was distributed ahead of the Conference.

SEMINAR 1: Purpose, period, scope

Moderator: Mr Jacques VERRAES, Senior Policy Official, DG Home Affairs, European Commission

Session One: Purpose

Mr. Verraes opened the seminar by asking whether, in terms of scope, the DRD is still an adequate instrument considering that criminals are using internet information services (ISS), and whether the scope of the DRD should be extended to cover the wider legislative space of Article 15 of the e-Privacy Directive 2002/58/EC, as some Member States have done, and whether viable alternatives exists to data retention.

Presentation by Mr. Kristian BARTHOLIN, Council of Europe (CoE), Criminal Law Division
Mr. BARTHOLIN questioned whether the purpose of the directive – that it is a tool to fight serious crime – is appropriate and adequate. The DRD is indispensable as a law enforcement tool, but access to retained data should not be unlimited.

'Data preservation', which is a tool introduced by the Cybercrime convention of the CoE, is often seen as less intrusive than data retention, Mr Bartholin stated, because it is targeted to a specific criminal investigation and provides a snapshot of what is going on at any one time. As such it provides good results when a suspect has been identified, but when there are no suspects this approach is not appropriate. It does not allow investigators to examine historical trends and patterns which can lead to the identification of the people involved in a crime. It could even be seen as more intrusive than data retention because under the Cybercrime Convention, data preservation allows examination of the content of communications.
Used properly, data retention and preservation can be complimentary methodologies – but proper safeguards need to be in place and there must be a test of proportionality and necessity. The fundamental rights challenge of data retention is that authorities can conduct investigations without prior evidence that a crime took place – this creates a risk of abuse. The purpose of the DRD must encompass the prevention of real danger as much as the investigation and prosecution of a specific criminal offence, not just addressing the abstract risk of crime. Under Article 8 of the European Convention on Human Rights, the test for the acceptability of interference by a public authority with the private information of an individual is that it is necessary, proportionate, has a specific and legitimate purpose, is executed in an adequate and relevant manner and does not constitute an inappropriate interference with privacy.

The problem is that the Directive lacks harmonised concepts, such as what constitutes a "serious crime" and who are "competent national authorities" so as to the answer the question of whether detective services should be able to access information. Further use of data by authorities should also be regulated; what is done with the information after it has been used, and when does it have to be deleted?

The DRD is an "indispensable tool" from the point of view of criminal law. A balance is needed between providing security for citizens and respecting their right to privacy. Therefore, strong safeguards are called for, Mr Bartholin stated.

Given the prevalence of internet services such as Facebook, the possibility of widening the scope of the DRD should be considered – but again, with proper checks and balances in place.

Presentation by Ms. Benedetta BUTTIGLIONE, speaking on behalf of Mr. Titziani MOTTI, MEP, European Parliament - Committee on the Internal Market

The internet offers ample opportunities for criminals,, for example the grooming of victims on Facebook by paedophiles, and exchanging of material that is tantamount to sexual abuse of minors. However, the privacy of citizens must be respected at the same time, as minors should be protected from technology-assisted crimes. In a resolution adopted by the European Parliament, the COM was asked to establish an early warning system at the European level, which would assist courts that are not always able to establish who uploaded certain illegal content online – as service providers are not obliged to store information about this kind of behaviour. In addition, service providers are not allowed to store the IP-addresses of destinations, i.e. the sites visited.

For email services, Ms Buttiglione stated, data protection levels are high and the legal tools to obtain traffic data in relation to the use of these services exist. It is different for Information Society Services such as online chat, and browser-accessed email services. She stated that the DRD should be extended to cover search engines, and to retain traffic and certain content data such as destination IP-addresses. Without providing for blanket retention such as with telecommunication traffic data, in this case the retention should be ordered by a competent authority (CA) within a certain time limit but which would be renewable. This approach could help prevent child sex crimes. As far as the DRD is concerned, it should only be extended to cover data relating to search engines for the purpose of preventing crime.

Dr. Hab. Andrzej ADAMSKI, Professor at Nicolaus Copernicus University, Torun, Poland

Professor ADAMSKI said there is no doubt that data retention is very useful for criminal investigations, but questioned whether it can be deemed "necessary" as required under the proportionality test. German research has shown that the data freeze regime, based on Article 16 of the Convention on Cyber Crime, is highly efficient, and that communications service providers have been able to satisfy the needs of law enforcement under this scheme.

However, some data is not covered by that alternative instrument. The proportionality test consists of three elements: suitability, necessity and proportionality *sensu strictu*. The most important element is the third one, because i.e. a regulatory measure can be disproportionate when the restriction it causes is out of proportion to the intended objective or to the result achieved. The crucial issue is the existence of checks and balances which would be totally neglected by some legislators.

Prof Adamski stated that 10 MS have opted for retention for one year for all categories of data. The Czech republic retains data for 6 months for internet access data and 12 months for telecommunication data. Italy, Malta and Slovakia also have different retention periods for internet data. The length of the retention period ranges from three years in Ireland, to two years in Poland and Slovenia, one and a half years in Latvia, and one year in Hungary - which unsuccessfully tried to implement a six-month retention period for unsuccessful calls.

In Poland there is no compensation to industry and there are no legal requirements for access to data – law enforcement has direct access. Polish law enforcement authorities generate a vast amount of requests for data. There is a need to build checks and balances into national legislation.

Mr. VERRAES clarified that the Directive was adopted as a first pillar instrument although it serves third pillar interests; the legal context changed under the Lisbon Treaty, which abolished the pillar structure and covers access to data and the modalities of use. In the course of the upcoming review of the Directive these issues will be considered. Mr. Verraes asked for Prof. Adamski's opinion on the suggestion that information regarding search engines should be covered by the DRD.

Dr. ADAMSKI said that a wider stream of data is necessary for investigating crimes, for example *Clickstream data*. The DRD currently only covers some types of communication. However, if for instance message services were included, this would open a Pandora's box – how far should we extend the scope of this instrument? The issue of proportionality should be considered first, and subsequently it should be decided whether or not to extend the Directive to cover other fields.

Mr. BARTHOLIN said there needs to be further harmonisation of the concepts used in the Directive. The Polish example (direct access by police) as opposed to access on the basis of a prior authorisation of a judge, shows this. However, checks and balances are needed both in the case of data preservation, and of data retention.

Caspar BOWDEN, Chief Privacy Adviser, Microsoft noted that the Cyber Crime Convention of the Council of Europe contains a legal provision on the expeditious preservation of computer data but there has been no enactment of provisions for the implementation of these powers. On the question of retention of data regarding the use of internet search engines, Mr. Bowden pointed out that searched content is not uploaded to search engines. He also asked whether MS had provided information allowing to break down the total number of requests in different data categories. Understanding patterns of access could help to understand the differences between the use of data retention powers by different MS.

Professor ADAMSKI said the question of scope/purpose is a delicate one. The use of data for the prevention of crime is outside of the scope of the Data Retention Directive but within that of the e-Privacy Directive. If there was an urgent need to prevent imminent danger to a given individual it should be possible and it would be justified to use retained data. However, the risk of cases such as the politically motivated investigation of journalists should be anticipated.

Jan Philipp ALBRECHT, Green MEP, European Parliament stated that from his point of view the picture of enforcement of fundamental rights across the EU is very fragmented. In the debate about data retention it seems that there is a focus on the necessity of the instrument in order to manage security interests, to the detriment of providing the appropriate protection of individual fundamental rights.

Mr. BARTHOLIN pointed out that it is up to individual MS to enforce fundamental rights; the Council only has the power to exercise pressure on MS to do this.

Mr. VERRAES clarified that the Commission's evaluation report is due in the first quarter of 2011. The information that COM has received from MS on the use of the different categories of data was published ahead of the current conference. The number of requests for subscriber data exceeds that of traffic and location data. In the Netherlands f.i. there is a dedicated database, containing up-to-date subscriber information, which is consulted up to 3 million times per year. In the UK 500,000 requests are made per year to obtain retained data, of which a substantial percentage are for subscriber information.

Ms. Vanna PALUMBO, Director of Garante per la protezione dati Personali, the Italian Data Protection Authority referred to the work conducted by the Article 29 Working Group, which she

said shows there is a big disparity between the obligations incumbent on commercial users to delete data on the one hand, and to retain the data for law enforcement purposes on the other. Ms. Palumbo asked whether the purpose of the Directive should be extended, and if so should the articles be further harmonised.

Mr. VERRAES highlighted that the current scope of the DRD covers only part of the legislative field of Article 15 of the e-Privacy Directive. The DRD introduced a conditional derogation of the obligation to delete. Mr. Verraes asked the panel for their views on whether further harmonisation of the scope of the DRD is necessary.

Ms. PALUMBO questioned whether referring to the e-Privacy Directive is a way of harmonising the legislative scope: the DRD has a narrower purpose than latter Directive but implementation of the DRD has been very patchy. "Competent authorities" for instance, should also be defined – does this include security services?

Dr. ADAMSKI said that secret services fall outside the scope of the Directive but they may be users of retained data. Considerable research is necessary to establish how national legislation transposing the Directive applies in practise – otherwise it is impossible to make a reasoned decision about the required changes to this instrument. The lack of definition of "serious crimes" for instance, means that the DRD can be used in either too broad or too narrow a sense. It is time to be precise.

Hielke HIJMANS, Head of Policy & Communications, EDPS agreed that a definition of *serious crime* is needed, and pointed out that it is also a problem that MS can use the same data for additional purposes. This possibility should be eliminated. If retained data can also be used for crime prevention it is, in his view, crossing a line – where is the limit? It would be helpful to find out how often MS use the instrument and how often it is used for a purpose outside the scope of the Directive – targeted research is needed.

Mr VERRAES confirmed that evaluation of the appropriateness of the use of retained data for the purpose of crime prevention under Article 15 of the e-Privacy Directive – is outside the scope of the evaluation. As to the 'necessity' of the instrument, Mr. Verraes highlighted that law enforcement authorities are requesting retained data millions of times per year. Having regard to the effort required to obtain data (in most MS a prior judicial authorisation is required) in conjunction with resource constraints, the fact that retained data is in high demand indicates that retained data has an edge that other crime investigation data does not have. MS would not go to such lengths to obtain retained traffic data if they would not be really necessary. Repealing the Directive is without effect because Article 15 of the e-Privacy Directive allows to maintain current national laws. An important issue for the upcoming review is the question whether the 'back door' of Article 15 e-Privacy Directive should be closed. This issue will probably not be part of the evaluation report.

The issue of **necessity of data retention** has been prevalent in this conference, and a wide range of viewpoints from the police, academic world and data protection community have been expressed. The discussion has shown that the Commission should find a middle ground between those who want to narrow the scope of the DRD and those who want to keep or extend the scope to provide security to citizens.

SEMINAR 1

Session Two: Period

Mr. VERRAES highlighted that under the Directive, the permissible period for data retention ranges from six to 24 months. MS have provided the COM with the following information on how

long information is retained. Italy retains telephony data for two years and internet data for one year, Malta retains telephony data for one year and internet data for six months, Slovakia retains fixed and mobile telephony data for one year and internet data for six months. Five MS have made other choices: Ireland retains data for three years, Poland and Slovenia for two years, and Latvia for one-and-a-half years. Hungary retains data for one year but data on unsuccessful calls is only kept for six months.

Mr. Jan-Philip ALBRECHT, **European Parliament (Greens/EFA), Committee on Civil Liberties** asked how *necessary* and *proportionate* data retention actually is? There are problems in the national laws of some MS, and there is public opposition to the DRD.
The purpose of the DRD was to fight serious crimes and terrorism, but data from MS shows that many cases where data is accessed do no relate to fighting serious crimes and terrorism; a clearer definition is required before allowing access to data. Access to data that is retained under the Directive should be authorised by a judge. The longer the retention period, the stricter the circumstances and conditions should be under which an authority can access the data. MS did not opt for such approach in their implementation of the Directive.

Under the Lisbon Treaty there is a new situation where common principles of law are laid down in the Treaty and also apply to data retention. Moreover the Charter of Fundamental Rights is binding on Member States, and the EU will become a member of the European Convention on Human Rights.
The trust of European citizens and the degree of acceptance of the DRD depends on the level of consistent implementation of fundamental rights and data retention safeguards. There should be minimum standards and safeguards, if not common principles, to build trust in the enforcement of these measures, and certainty about the circumstances where authorities can access information. Data retention requires co-operation between police and justice authorities throughout the EU. The problem is not just the relation between the freedom of the individual and the powers of the State but also the fragmented nature of legislative and constitutional frameworks within the EU.
Mr Albrecht called for the Directive to be overturned, and for alternative measures to be found which are compatible with the EU Charter for Fundamental Rights.

Professor ADAMSKI noted that most MS have opted for a one year retention period; this could indicate that a common period of retention might work. Currently there does not seem to be any single factor accounting for the difference in choice. It is not related to the prevalence of crime or of specific types of crime in countries such as Italy, Ireland and Poland, which opted for the maximum period. Neither does the effectiveness of law enforcement authorities explain MS' choice. If a criminal is the subject of an investigation abroad, then law enforcement in the home country must apply the standards of the foreign MS to determine the conditions for access and use. He wondered whether a risk existed of forum-shopping?

Mr. VERRAES said that less than 1% of requests for retained data are for data retained in another MS, so the concept of forum-shopping seems far-fetched. The idea of centralised data storage has been discussed in the DRD Expert Group; this raises the question of which data retention period should be applied – that of the country of origin of the data or of that where the information is stored?

Mr ALBRECHT said that it is not only a question of how long data should be stored, but also of the necessity of doing so. What should be the criteria to judge necessity – lowering crime rates or improving the number of crimes cleared? In Germany, before the DRD there were clearing rates of over 80% for internet crimes and child abuse material – this is far above the average clearing rate for crime which is around 50%.

Mr. VERRAES stated that the first issue to assess, on the basis of the necessity test, is whether we need retention, and subsequently how long the retention period should be. Without data retention, some crimes would not be solved. However, the replies from MS showed that more than 70% of data requested is younger than six months; this seems to indicate a possibility of having a lower limit for data retention.

Mr. ALBRECHT pointed out that the DRD states data retention should only be used to combat serious crimes and terrorism. However, the worst criminals would also have the best technological capabilities to escape those measures - which means they are not justified. Also, a small amount of cases are justifying a measure which is intrusive on the entire population.

Mr. Luc BEIRENS, Head of the Belgian Federal Computer Crime Unit (FCCU) provided FCCU figures showing a correlation between the length of the retention period (of internet related data) and the number of crimes that can be solved by using this data. In 2007, for IP-addresses with a retention period of six months, 15% of crimes could be tackled, while at one year retention period, answers were given for 66%, and at 18 months, 84%. At two years, the rate was 97%. For IP-addresses a date and time can (and must) always be given, but this is not the case for telephone numbers. Although Belgium has not yet fully transposed the directive, data are obtained from billing and marketing records.

Mr. ALBRECHT said data obtained from billing and marketing, is stored on the basis of consent being given by users to companies. Under the DRD the data is mostly obtained without the consent of the data subject. In response to a comment that data exists with or without consent (i.e. data found in household waste) Mr. Albrecht emphasised that it is a core right to clean up one's own rubbish and this should not be prohibited.

Mr. VERRAES clarified that the public interest (e.g. to fight crime) may be a legitimate reason to use data that is stored without consent. The conditions for access and use are outside the scope of the Directive, and subject to relevant national legislation. At this stage the COM has only taken MS to court for not transposing the directive, not how they transpose. The police and the state need data, and the longer the retention period the more crime can be solved. For companies there would be no basic difference between retaining data for billing or under mandatory data retention.

Ms. Cristina VELA MARIMON, Senior Adviser, Telefónica, S.A., Spain disagreed and said that less data is generated for billing/marketing purposes than is retained under the Directive, because different and dedicated systems and databases are needed for storage.

Mr. VERRAES pointed out that very few MS have passed legislation on mandatory reimbursement of capital expenditure by companies to purchase equipment to retain and retrieve data. This issue will be considered in the context of the review of the Directive, but he questioned whether MS would be prepared to foot such a bill in these economically difficult times.

SEMINAR 1

Session Three: Scope

Mr. VERRAES said that the countries in the European Economic Area (Norway, Iceland and Lichtenstein) should also adopt legislation to transpose the DRD. Iceland and Lichtenstein have already done this, and Norway has prepared legislation that will shortly be presented to the Norwegian Parliament. There is strong political debate around this. The current Norwegian law allows law enforcement authorities to order the conservation of communication data; the question is whether this system is sufficient?

Presentation by Rune Utne REITAN, Detective Superintendent/Chief Investigator, National

Criminal Investigation Service – Norway:

DS REITAN presented the Norwegian approach to data preservation (data freeze) from the perspective of the Norwegian police. He highlighted that data freeze is not an alternative to data retention. Norwegian rules regulating data freezing are based on the Convention on Cyber Crime; Article 16 of the Convention requires MS to regulate the temporary securing of stored data. There was no Norwegian legislation on expeditious data preservation until 2005. No general obligation exists for ISPs to store (all) data. Therefore, only data which exists when the freezing order is issued, and specified by law, can be the subject of such an order. Under Norway's Criminal Procedure Act, the data has to be specified and can only be frozen for a certain time – but this can be extended.

For data freezing to work, data must be retained or there is nothing to freeze. Police also need to know at an early stage what data might be of interest. All law enforcement investigation is reactive by nature: investigators have to go back in time and reconstruct events that led to the crime. IP logs are stored for a maximum of three weeks, and many ISPs do not store data at all. Telephone traffic data is typically stored for three to five months. However, among ISPs the trend is now to store less and less traffic data. By the time police know what data to request it has usually been deleted.

Data freezing is a very useful way of obtaining electronic evidence which would otherwise be deleted; it allows authorities to substantiate the involvement of another suspect or family. Data freezing is not an alternative to data retention; they are complementary: data retention is a pre-requisite for freezing.

Dr. ADAMSKI expressed his view that the 'psychiatric approach', meaning the use of anecdotal examples to construct a generality (which is the approach to justify the directive) is not the right approach. Professor Adamski gave the example of Canada opting for preservation orders rather than a data retention regime – with more demanding requirements for access to historical data than for the real-time tracking of the movements of a suspect.

Dirk HENSEL, Legal Counsel, BIDI – Federal DPA Germany highlighted that Germany has not yet re-implemented the directive. It is currently discussing quick freeze. He confirmed that police are a reactive force but wondered how long the reaction span should be to justify a certain retention period?

D.S. REITAN said the Norwegian Police advises one year.

SEMINAR 2: Modalities, authorities, operators

Moderator: Ms. Cecilia VERKLEIJ, Head of Sector, DG HOME A3, European Commission

Session One: Modalities

Presentation by Mr. Charles MILLER, Senior Manager, ACPO Communications Group (UK):

Mr. Miller explained that he is a serving police officer in the UK since 1993, has focussed specifically on communications data used retrospectively in the investigation of crime. Communications data is vital to criminal investigations and prosecutions, he emphasised, but problems are arising as a result of the growth in modern communications - especially mobile telephony. For example, downloading all registered data from high-tech mobile telephone devices can take up to 50 hours, whereas with older models of standard mobile phones it only took around

30 minutes.

Police officers in the UK do not have unlimited access to data: in order to acquire data for a criminal case, they have to refer to a Single Point of Contact (SPoC), which acts as a type of "guardian gatekeeper", ensuring that public authorities act in an informed and lawful manner. Under the SPoC system, a senior police officer is responsible for the oversight of the acquisition and use of data within the police force and public authorities, and for external use, a High Court Judge and a team of trained officers is responsible. Access to data has to come through this system of proportionality oversight at the highest level, and under the control of an interception commissioner.

While human rights must be protected, there are also strong fiscal constraints, because in the UK the State pays for the retention of data and for the retrieval mechanisms operated by independent and private service providers.

Mr. Kurt Sejr HANSEN, Chief Information Security Officer, TDC Denmark explained that he is in charge of implementing the Data retention Directive at TDC. The Danish government passed a bill on data retention in 2006 and operators had one year to implement it. There were many challenges involved in implementation, including the skills required to keep up with the pace of technological developments, and the costs entailed for operators who are sometimes required to provide data less than one hour old.

Mr. Hansen also pointed out the practical difficulties and costs involved in providing data linked to 'session log,' which requires operators to save data in every 500 incoming ID packages. This is expensive and takes up a huge amount of space: about 3 terabyte per year, which needs to be compressed and thus requires a long search time. However, while session log is a requirement, in the three years since implementation there has been almost no use of it by law enforcement authorities (LEAs).

Within LEAs there are knowledge gaps when it comes to the use of retained traffic data. At the higher levels there is good knowledge, but lower down there is a lack of understanding of the technical complexities involved in retaining, providing and using data. LEAs are not well prepared to receive and use the technology effectively. There is also a lack of formal incentive to be efficient in certain areas within authorities.

In the Nordic area, which is the relevant market for Denmark, there is a lack of uniformity. There is an urgent need to connect law enforcement systems within this region, in order to provide legal, affordable and quick access to retained traffic, location and ID data.

Mr. Herke KRANENBORG, Legal Officer, Office of the European Data Protection Supervisor said that the ideas of data retention and data access cannot be separated, and therefore the DRD should contain both. He drew the attention to discrepancies between national systems of data retention in different MS, and referred to the UK example of best practice exchange as a useful tool - while noting there was still a need for greater cross-border harmonisation. Mr Kranenborg backed the idea of a single access point as a way of ensuring faster processing of data, and improving control of access, but he emphasised the need for the whole chain of actors involved to comply with the system. There also needs to be a discussion on cross-border transfer of data, and cohesive agreement on a clear definition of what constitutes serious crime, as well as agreement on what should constitute an acceptable retention period.

Mr. Christof TSCHOL, Institute of Human Rights in Vienna expressed concern over who has access to data.

Ms. Cristina VELA MARIMON, Senior Adviser, Telefonicà (Spain) highlighted a general lack of training provision. Spanish judges are now being trained, she highlighted.

Ms. Alina BARBU, Chief of Service, Romanian Ministry of Justice asked how long data can and should be retained, and whether once the retention period is over, operators can continue to use the data and share it with authorities if requested?

Mr. HANSEN said that in the case of TDC Denmark, if data is available it will be shared on request, although this is not an obligation once the period of retention is over. Operators keep data for billing requirements, whereas location-related data is not retained for commercial use outside the enforceable period of retention.

Mr. MILLER expressed his view that regarding costs, it is not data retention but data retrieval that creates the real financial burden. In the UK, data retrieval accounts for about 85% of costs.

Mr. Peter DUNN, Analyst, Cullen International said that there is a need for analysis of retrieval periods. Referring to Mr. Hansen's point on the need for cross-border harmonisation in the Nordic region, Mr. Dunn questioned how, where and for how long data could be stored in a cross-border context.

Ms. VERKLEIJ summed up the discussion by highlighting the potential of the UK's SPoC model, and questioned how this could work in terms of authorisation; whether prior authorisation would be required, or whether it would be granted retrospectively. What level of independence would be required of the authority granting such authorisations? This needs further definition. Ms. Verkleij also noted that there is common view among industry and law enforcement agencies that there is a strong need for further education of LEA staff working in the area of data retention.

SEMINAR 2

Session Two: Authorities

Alina BARBU, Chief of Service, Romanian Ministry of Justice focussed on the notion of competent authorities, and the challenges faced by Romania in implementing the DRD. The main issue for Romania was the question of obligations, and the need under the Romanian constitution to fully respect the rule of law on human rights. There was also a question over who should be the competent authorities – there is a need for clearer guidance on this. On the notion of prevention, which is only mentioned in the preamble to the DRD and not in the main text, Ms. Barbu suggested that the directive had been adopted in the context of the better functioning of the internal market. There are cultural differences regarding the notion of prevention. Regarding cross-border transfer of data, there are many different authorities involved, which raises questions around the purpose of the instrument; is it for use within the internal market, or more for law enforcement use?

Mr KRANENBORG said that databases at the EU level are overloaded and that there is therefore a need for the COM to provide an overview of existing instruments as early as possible in 2011. Regarding the management of these databases, Mr. Kranenborg felt that the definition of competent national authorities is currently too broad. In particular, because data retention is ultimately concerned with 'secret surveillance', EU citizens need to have a clearer idea as to which bodies have authority, how they can use it, and for how long. Mr. Kranenborg also highlighted the need for clearer definitions on what constitutes an authority and serious crime, and on the scope of the directive - taking into consideration the huge differences between national authorities.

Christof TSCHOL highlighted his concerns over 'enforceability' regarding human rights, and whether the police would have access to private IP-addresses, because there is a concern for citizens

over what can happen to private data; can the police gain access for their own purposes outside the framework of the DRD?

Gero NAGEL, AK Vorrat (Germany) asked whether there was really a need for the Directive, suggesting that it could only be used to focus on 'small' crimes because terrorists and high level organised criminals know how to beat the system and remain anonymous. It is relatively easy to use the internet without leaving a trace, he noted.

Ms VERKLEIJ disagreed, and said that experience has repeatedly shown that people always leave some kind of trace. This statement was supported by Ms. BARBU, who said the authorities are always ahead in this respect.

Mr. MILLER returned to the question of 'enforceability', expressing his opinion that need a strong legal instrument is needed in the EU in order to protect the general public, because its data is available and so there is a need to set up a framework of data protection under the directive.

SEMINAR 2

Session Three: Operators

The focus of the final session of Seminar 2 was operators under retention obligations. Under the current directive, obligations apply to the providers of publicly available electronic communication services, or of public communication networks.

Ms VERKLEIJ asked participants to consider whether a potential new proposal should specify which operators are subject to retention obligations, and if yes, which criteria should inform the choice of operators under retention obligations?

Presentation by Mr. Luc BEIRENS, Head of the Federal Computer Crime Unit of the Belgian Ministry of the Interior:

Mr. Beirens began by asking what risks surround the definition of operators, what expectations surround law enforcement - who has the obligation to enforce the law and who (which companies) should be excluded from it?

Mr. Beirens argued that operators have to tread a fine line regarding obligations on data retention; if they do not keep it, they can be punished, while if they do but do not follow the Directive they can also be punished. Therefore, there is a need for far more clarity on these requirements. If all operators are not included, then it would be fair to assume that criminals will shift towards those not included. However, if all operators are included, the smallest operators may not be able to meet the financial demands of such an obligation.

The definitions in the directive are too vague, Mr Beirens believed; both the definitions and the terminology used need to be clearer. Under the 2002 Directive on Billing and Marketing, if there is a national law on data retention, then information may be stored, if not then the operator is obliged to wipe out all traces.

Mr. Beirens disagreed with the suggestion from earlier in this seminar discussion that criminals will switch to hidden services. He said most criminals do not have advanced technological skills – although some do and therefore there could be a need to expand the directive to cover certain loopholes such as forensic analysis and internet access.

Summing up this last panel session for Seminar 2, **Ms. VERKLEIJ** highlighted the need to qualify which operators are obliged to retain data, taking into consideration the issue of 'big versus small' operators – and the financial burden smaller operators could incur.

SEMINAR 3: Crime, costs, data security

Moderator: Mr. Achim KLABUNDE, Head of Sector from the European Commission's Directorate General for the Information Society (Unit B1)

Session One: Crime

Alexander Alvaro, MEP (ALDE), member of the European Parliament's Civil Liberties Committee argued that a new DRD should have a clear catalogue, as exists for the European Arrest Warrant (EAW), with a limited number of crimes and minimum/maximum punishments, to allow for coherence among LEAs and to give legal certainty to LEAs and telecoms operators so that they know under what circumstances they can hand over data.

There are various differences between EU Member States with regard to their implementation of the directive (e.g. Germany had 2,600 requests compared to Poland's one million requests in 2009).

Mr. Alvaro noted that there is a discussion on the possibility of extending the directive to cover the results of queries in search engines, or crimes like illegal downloading (for example of music) but argued that this was never the purpose of such an 'invasive' instrument. He hoped that the COM would resist including all sorts of crimes in the directive in its revision.

Mr. KLABUNDE said that the COM had suggested to the Council that the EAW should be taken into account as a catalogue for serious crimes when implementing the DRD, but that the suggestion had not been endorsed.

Francis STOLIAROFF, French Ministry of Justice argued that France has always considered that the DRD is not limited to serious crimes, but also covers other offences. He cited nuisance phone calls as one example of such an offence.

France is deeply hostile to any reduction in the scope of the directive, Mr. Stoliaroff emphasised. France believes that that it would be useful to harmonise the length of time data must be retained, setting this time at one year. He argued that, even without the Directive, data would be kept by operators for six months for billing purposes. In his view, one year or two years delivers a real additional benefit.

Gert WABEKE, Manager of Lawful Interception, Royal KPN (Netherlands), and member of the Expert Group on Data Retention, said that there are enough instruments to combat stalking or other crimes from communications devices, such as the 'quick freeze' procedure. The difficulty with *cyber-mobbing* is that, if the offender is sophisticated, (s)he would use an internet café in order to ensure that they are difficult to trace. Mr. Wabeke suggested that another instrument could be used to solve this sort of crimes.

Mr. STOLIAROFF said that it is important to be able to identify people when they are on the internet. In France, customers using internet cafes have to provide their name and identity, so they are not totally anonymous.

Mr. Michael EBELING, member of AK Vorrat Hannover said he did not understand why data needed to be stored for two years for cases of suicide or nuisance calls. He suggested that a

distinction should be made between current (real time) interventions (e.g. suicide) and information on terrorist plots.

Mr ALVARO drew attention to the risks of illegal access to data and abuse, or even of WikiLeaks publishing everything. He stressed that the use of data generated by tools of a highly intrusive nature need to be limited to crimes such as murder and terrorism. He did not see stalking as being at the same level as murder or setting up a terrorist organisation.

Mr HIRSCH (HO UK) said that for malicious communications (for example, people dialling the UK emergency number 999 or the 112 emergency number when they did not need the service), the UK needed to be able investigate that type of crime and identify the person. He suggested that adding a definition of 'serious crime' might lead to a situation in which certain crimes would not be investigated because of the Directive.

Mr ALVARO argued that, just because data is out there, it should not all be open to all public prosecutors.

Mr KLABUNDE pointed out that Article 15 the E-Privacy Directive takes care of the needs of LEAs regarding prevention of crime. The issue what added value is the clear cut obligation to retain certain data which DRD provides in addition to this.

SEMINAR 3

Session Two: Costs and reimbursement models

French reimbursement model

Presentation by Francis STOLIAROFF, French Ministry of Justice:

France pays a fee to meet the costs incurred by operators when providing LEAs with requested data, the maintenance of software and the payment of staff in charge of looking for the data.

It has created a confidential reference document for police and legal authorities. They can either make a request for data electronically (in which case the cost of requesting a phone number is 0.65 cents per request) or by letter (in which case it is 6.5 Euro per request).

Through this service, LEAs can, for example, identify whether a public phone was used and can identify the date, time and length of each call. Data on calls made on a foreign mobile phone in France can also be found as the data is stored with the operator in France as well as with the foreign operator. The fee is paid by the convicted person.

UK reimbursement model

Henry Hirsch - United Kingdom Home Office:

In the UK, a notice is sent to the operator telling them that they must keep certain data This notification helps operators to consider what tools they will need in order to do this, and what they will cost.

In the UK, the capital costs are borne by central government, while the operating costs are borne by the public authorities using that data (e.g. law enforcement authorities) on a *per usage* basis. By

paying, the idea is that the UK government can set standards and can negotiate these with the operators. For example, the UK can set standards for:
- Data security and handover: by paying for secure connections between operators and the police network, the loss or poor transmission of data can be avoided
- Disaster recovery standards
- The security clearance of staff accessing the data
- Response times

Understanding the real cost of such a service can help public authorities make sensible decisions such as whether to spend money on retrieving this data or, for example, spend it on surveillance teams or a new police car.

Mr. WABEKE stressed that operators are not looking to make money from this service, but they do want costs spread out reasonably. Good communication between operators and law enforcement authorities was necessary, he said.

Mr. KLABUNDE said that the DRD cannot provide an answer on the obligations of a company's switchboard to identify the extensions of callers within the company.

Mr. ALVARO referred to a European Parliament study on running costs (for data retention), which, depending on the size of the service provider (and whether they also offer internet services) showed that costs can vary from one million to one hundred million Euro. He questioned whether it was the right approach for governments to set an obligation, and then make industry responsible for the costs involved.

Mr. STOLIAROFF expressed his belief that France reimburses the extra costs incurred by companies in connection with data retention generously, and that operators are in no way losing out.

Mr. KLABUNDE pointed out that the COM had asked MS in a declaration (which is not legally binding) to set up appropriate reimbursement systems.

Chris SHERWOOD, Director of Public Policy at Yahoo! Asked if cost reimbursement should apply to legal advice too. He referred to a case in Germany in which operators have been obliged to shut down data retention compliance solutions due to a court judgement.

In response to a question on how many operators do not comply with requests for data in France, **Mr. STOLIAROFF** said that operators are legally obliged to reply and that he was not aware of any cases where they have refused. He added that, generally, MS are obliged to ensure that citizens are safe, and therefore to meet the costs of justice procedures. However, he added, the issue of who meets these costs should be clarified.

Mr HIRSCH said that it is possible that there are operators with whom the UK is not in touch, but the UK does try to work with operators. He stressed the importance of not placing too great a financial burden on operators, as this could lead to their cutting spending on security. The UK wants to be able to call up an operator in the middle of night if there is a threat to an individual, and Mr. Hirsch argued that paying for services allows the UK to have that approach.

SEMINAR 3

Session Three: Data Security

Vanna PALUMBO from the Italian data protection authority gave a presentation of an

assessment by the Working Party of Article 29 of the Data Protection Directive, in which the European Data Protection Authorities assessed the compliance of private operators with the data protection requirements laid down in the DRD at the national level. The key points of the assessment were:

- If the costs are only borne by service providers then they will have an impact on security measures
- A physical separation between billing data and data available for law enforcement purposes is very important as it can ensure that the purpose of the DRD is not exceeded
- The DRD obliges operators to retain information even on people who are not suspects – safety measures are needed to avoid abusive use of this data
- The DRD cannot extend the conditions and obligations of the e-Privacy Directive
- The DRD has been implemented differently in different MS (e.g. access to data is sometimes direct, and in other cases has to be done using specialised staff and security codes)

The assessment recommended establishing a standardised European procedure for the access to and handover of data, so that it is clear how a request should be formulated and how it has to be filed – specifying the time schedule, places and people involved. This could improve the accountability of authorities as they would then be obliged to clearly state what they want, and also give reasons for their requests.

Jonas BREYER from the German working group against data retention (AK-Vorrat) pointed out that the German Constitutional Court has ruled that the national law transposing the DRD was unlawful. Strong encryption and rules on who may access the data are areas where the Court sees the directive as being insufficient. He argued that the Directive disregards Article 8 of the European Charter of Fundamental Rights. He also argued that the DRD had not helped cut crime, pointing to German federal crime statistics which showed that 79.8% of internet crime cases had been solved in 2008 (i.e. without the DRD) and that 75.5% of internet crimes had been solved in 2009 (i.e. with the DRD).

CLOSING SESSION

Speech by Cecilia MALMSTRÖM, European Commissioner for Home Affairs:

Commissioner Malmström said that while a wide range of views are held on the DRD, most participants in the conference were likely to share the same basic concern that citizens can feel secure, while at the same time their rights to privacy are protected. She highlighted that she is convinced of the need for data retention for law enforcement, since telecommunications data can be the only way of detecting and prosecuting serious crime - but the Directive has to be changed. The Commissioner questioned what form data retention should take, and how to avoid abuses of data retention.

The COM's evaluation of the directive so far has highlighted four important points:

1) On the usefulness of retained data: national authorities very often request access to this data. 2008 – 2009 figures from 20 MS show an average of 148,000 requests per year in each MS. 90% of that data was less than six months old when the authorities asked to see it. The information provided showed that many criminal investigations would not have been successful without this data – in one MS retained data was used by LEAs in more than 86% of cases resulting in criminal prosecutions.

2) How have MS implemented the DRD?: 20 MS have implemented it and several others are

expecting to do it soon. If necessary the COM will take action before the ECJ to ensure the DRD is implemented. However, the DRD has not been implemented in the same way in every MS. Differences exist on the length of retention periods, the purposes for which data can be accessed, and which authorities can access them. These variations are due to the fact that the provisions of the directive are formulated in an open-ended way.

3) Costs of data retention for economic operators: It does not seem that the telecoms sector has been negatively affected by the directive. However, differences in implementation in different MS may mean some operators are more seriously affected. Should there be clear rules on state compensation?

4) The impact of the DRD on fundamental rights: The retention of data is a source of concern for citizens, although there is no evidence it has led to abuse in any concrete cases.

Commissioner Malmström stated that the DRD is here to stay but there is room for improvement.

Therefore, building on the evaluation report which should be published early next year, the Commissioner announced that she will prepare a proposal to amend the Directive. This proposal should cover the issues of purpose and types of crime covered, harmonised and possibly shorter retention periods, the authorities who will have a right of access and the type of data that can be accessed and according to which procedures, whether operators should be compensated by the State, and what types of data to retain. However, the Commissioner was sceptical about enlarging the scope of the directive, as suggested by the Parliament in a written declaration. She also expressed her belief that data freezing is not a convincing alternative as it cannot bring back deleted data. There are no short-cuts.

Report of the three panel moderators

Jacques VERRAES, moderator of SEMINAR 1:

There is no doubt about the need for data retention, but the question is under which conditions it should be permitted. The real question is whether the DRD is necessary in a democratic society. Data preservation allows the retention of data available for billing and marketing purposes, while the DRD allows the deliberate retention of data for law enforcement purposes. According to telecoms operators, shorter retention periods and less data could still provide the police with relevant information. Data retention is a prelude to data preservation, they are complementary; if the target is unknown, it is unclear which data should be preserved. The police force is reactive – reacting to crimes which occurred in the past. There is scope for improvement e.g. on cross-border exchanges of retained data. An issue to be examined is whether a harmonised regime to order (cross-border) data preservation would reduce the need for data retention. The upcoming review of the Directive could usefully consider narrowing the variance of national conditions for access and use.

Cecelia VERKLEIJ, moderator of SEMINAR 2:

The Seminar discussed three issues; modalities, authorities, and operators. The conclusions on modalities were: how would a single point of contact (such as in the UK model) work in terms of authorisation? Would prior authority be needed, and if yes, how independent would the authority granting it be? There is a clear need for education of law enforcement authorities about the conditions for access to and use of retained data.
On the issue of authorities there was one conclusion: defining which authorities should have access

to retained data is closely linked to other issues. E.g. if the Directive gave a clearer definition of which crimes are covered, that would have an impact on which authorities would have access to data. If the future Directive covered prevention, this would also affect which authorities had access to data. On the issue of operators there was general consensus that further examination and clarification is needed regarding which operators are obliged to retain data. One particular issue is the question of big versus small operators; this is a very complicated area.

Mr. Achim KLABUNDE, moderator of SEMINAR 3:

In the 'crime' session the discussion focussed on the threshold for serious crime, and whether the Directive should be limited to serious crime. Many crimes cannot be investigated because there is no access to retained data. However, this concern of LEAs and government was opposed by civil society representatives who said that if the DRD is extended to cover other types of crime, then how can limits be set to avoid ending up with full data supervision all the time? In the 'cost' session two different approaches were discussed; in France, the convict pays for all criminal enforcement measures, while in the UK the State pays for data for law enforcement purposes. In the 'security' session the outcome of the Article 29 Working Party evaluation was discussed. The working party assessed how measures work in practise and found a huge diversity of measures and variations in levels of security. It said that procedures should be further harmonised. On the risk of misuse of data, the seminar heard of one case of retained data being manipulated by an employee who had personal relations with the criminal being investigated.

Closing discussion between panel moderators and audience

Key points made by the audience included:

Is an EU instrument really necessary considering that MS are calling for subsidiarity and there is currently no harmonisation of procedures?

The directive states that data should only be retained once; MS should pay closer attention to this.

On abuse of the DRD, a representative of a Polish NGO, said it had reported many cases of abuse – for example one case where the DRD has been used to reveal journalists' sources. The Commission said it has not received any feedback on abuse, and the Article 29 Working Party did not signal any cases of abuse. This was challenged by Caspar BOWDEN who said that the Article 29 report refers to instances of the content of communications being retained, to the retention of URLs of web pages, and to statutory retention periods being massively exceeded.

On safeguards, the Commission questioned whether there should be a harmonised scheme of safeguards for data protection or whether this should be left up to MS. Jan Philipp ALBRECHT stated that if MS fail to set up safeguards and as a result access to data is allowed in fields other than serious crime, this in itself constitutes abuse. The EU should take this up with MS - otherwise an EU-level approach does not work. The Commission said that the DRD does provide safeguards, since it is based on the e-Privacy Directive of 2002, which in itself is based on the 1995 Data Protection Directive, and the safeguards provided for in these two instruments fully apply. However, the problem is the implementation of legislation – and the Commission cannot enforce without concrete indications that the DRD was ill-transposed.

Data-mining must be avoided.

Concluding remarks by **Reinhard PRIEBE, Director, DG HOME, European Commission:**

The Commission is relying on input of stakeholders to produce a successful evaluation report, therefore this conference has been very useful. The discussion on data retention is extremely relevant in terms of fundamental rights. The DRD could be seen as a test-case in achieving the right balance between security needs and respecting fundamental rights, particularly data protection rights – this is a very difficult task and the COM is relying on outside expertise and input to get it right.

Mr Priebe thanked all participants for their attendance.

ENDS

Jacques Verraes, DG HOME

Annex 1

List of abbreviations

CA = Competent Authority
COM = European Commission
CSP = Communication Service Provider
DRD = Data Retention Directive
EPD = E-Privacy Directive
ECJ = European Court of Justice
ECtHR = European Court of Human Rights
ECHR = European Convention on Human Rights
IP = Internet Protocol
ISP = Internet Service Provider
LEA = Law Enforcement Authority
MS = Member States

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR HOME AFFAIRS

Taking on the Data Retention Directive

Data Retention Conference,
25 November 2010, Brussels

DISCUSSION PAPER FOR PARTICIPANTS

Background

Under Article 14 of the Data Retention Directive[1] (hereafter "Directive"), the European Commission was required to submit to the European Parliament and the Council no later than 15 September 2010 an evaluation of the application of this instrument and its impact on economic operators and consumers, taking into account further developments in electronic communication technology and the statistics provided to the Commission with a view to determining "whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data [covered] and the periods of retention."

As the statistics provided by Member States proved insufficient for the completion of its evaluation report, the Commission requested a second round of data in the summer of 2010. This new information should enable the completion of this report by early 2011.

Review of the Directive

The ongoing evaluation process and recent developments in various Member States have persuaded the Commission to consider a *broad* review of the provisions of this Directive, extending beyond data coverage and the length of retention periods.

Its internal reflection has focused on the following nine variables. Below the description of each variable, readers will find a number of questions for further discussion:

(1) **Purpose of data retention**. Data retention seeks to enable competent national authorities to investigate, detect and prosecute serious crime, as defined by each Member States in its national law. The e-Privacy Directive,[2] under Article 15, permits data retention for safeguarding national security, defence, public security and for preventing, investigating, detecting and prosecuting criminal offences or the unauthorised use of electronic communications systems.

- Does the expedited preservation of stored computer data[3] (known as 'data preservation' or 'quick freeze') pose a viable alternative to data retention?
- Are there any other viable alternatives to data retention besides data preservation?
- Should a potential new proposal on data retention have a broader purpose (similar to Article 15 of the e-Privacy Directive) or a narrower one?

[1] Directive 2006/24/EC, OJ L 105, 13.4.2006, p. 54
[2] Directive 2002/58/EC, OJ L 201, 31.7.2002, p. 37
[3] Council of Europe Convention on Cybercrime [Article 16], Budapest, 21.XI.2001, ETS 185

(2) **Scope**. The Directive covers electronic communication traffic and location data, as well as information on subscribers and registered users. It expressly forbids the retention of data relating to the content of electronic communication.

- Should a potential new proposal include Information Society Services (ISS)?[4]

- Should the data on subscribers and registered users be treated the same way as traffic and location data?

(3) **Data retention period**. The Directive obliges Member States to ensure that data are retained for a minimum of six and a maximum of 24 months.

- Should the maximum retention period be different from 24 months?

- Should the minimum retention period be different from 6 months?

- Should there be a single retention period for all categories of data covered by a potential new proposal?

- Should there be different retention periods for mobile telephony, fixed telephony, internet data (including internet access, internet e-mail and internet telephony) and, if they are included in a new proposal, Information Society Services?

(4) **Definition of serious crime**. The Directive leaves it to Member States to define 'serious crime' to which retention obligations apply.

- Should a potential new proposal take the list of serious criminal offences set out in the European Arrest Warrant as the basis of its own definition?[5]

- Should a potential new proposal take the list of serious criminal offences set out in the Europol Decision as the basis of its own definition?[6]

- Should a potential new proposal base its definition of serious crime on Article 83 of the Treaty on the Functioning of the European Union (TFEU)?[7]

- Should a potential new proposal develop its own definition of serious crime?

(5) **Authorities with access**. Under the Directive, competent national authorities may access retained data in specific cases and in accordance with national law.

- Should a potential new proposal specify the type(s) of national authorities with access to retained data?

(6) **Mode of access and cross-border transfer**. The Directive leaves it to Member States to define the procedures to be followed and the conditions to be fulfilled by competent authorities to gain access to retained data.

- Should a potential new proposal regulate access to and the cross-border transfer of retained data?

---

[4] Directive 98/34/EC, OJ L 24, 21.7.1998, p. 37

[5] Council Decision 2002/584/JHA [Article 2(2)], OJ L 190, 18.7.2002, p. 1

[6] Council Decision 2009/371/JHA [Annex], OJ L 121, 15.5.2009, p. 37

[7] Article 83, TFEU defines particularly serious crime with a cross-border nature as follows: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

- Should a potential new proposal stipulate that an independent authority, such as a national contact point, shall receive, vet and authorise domestic access to and the cross-border transfer of retained data?

- Should it stipulate that a judicial authority shall authorise domestic access to and the cross-border transfer of retained data?

(7) **Operators under retention obligations**. Under the Directive, data retention obligations apply, within the jurisdiction of the Member State concerned, to the providers of publicly available electronic communication services or of public communication networks.

- Should a potential new proposal specify the operators under retention obligations?

- If yes, what criteria should inform the choice of operators under retention obligations?

(8) **Cost recovery**. The Directive contains no provisions on the potential recovery of costs incurred by operators in connection with data retention, yet several Member States have implemented such schemes.

- Should a potential new proposal contain a cost recovery scheme for operators under retention obligations?
- If yes, should such a scheme extend to capital and/or operational costs incurred in connection with data retention?

(9) **Data security**. The Directive sets out some basic provisions concerning data security.

- Should a potential new proposal specify in greater detail the data security obligations incumbent upon operators and authorities?

- Should it require the mandatory logging of users?

- Should it define a state-of-the-art data security regime similar to that included in the Prüm Decisions?[8]

European Commission, DG Home Affairs, October 2010

[8] Council Decision 2008/615/JHA [Article 29], OJ L 210, 6.8.2008, p. 1; Council Decision 2008/616/JHA, OJ L 210, 6.8.2008, p. 12