EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

Directorate F : Security
Unit F3 : Police co-operation and access to information

Brussels,
JLS F3/JV D(2009) 9330

REPORT OF THE DATA RETENTION CONFERENCE, 'TOWARDS THE EVALUATION OF THE DATA RETENTION DIRECTIVE', BRUSSELS, 14 MAY 2009

The meeting was attended by some 140 participants, and speakers made up of representatives from law enforcement authorities (LEAs), ministries, national and European Data Protection Authorities, industry, academics, and representatives of civil society, NGOs, the European Commission and other European Institutions. The aim of the conference was to start the process of evaluation of Directive 2006/24/EC ('the Data Retention Directive' or DRD) mentioned in Article 14, namely to assess whether the Directive fulfils its purpose. The idea was also to look at to what extent the data retained under the conditions set out by the Directive allows law enforcement authorities to detect, investigate and prosecute serious crimes whilst keeping the balance between efficiency, the privacy of citizens whose data are processed and the economic impact on service providers. The conference will provide COM with input for the evaluation report that it has to present to the Council and the European Parliament by15 September 2010.

SUMMARY

The DRD is being used by many LEAs of MS. MS need to demonstrate, in the course of the evaluation, including by means of statistics that the retention of data under the DRD is necessary and effective to fight organised crime and terrorism and justifies the impact it has on fundamental rights.

The following conclusions emerged from the discussions.

- Data protection and privacy issues

1) Effective protection is not yet fully in place concerning storage, security measures applicable for retention, and access conditions.
2) There is a lack of knowledge about the impact of implementation on companies and individuals.
3) Need exists to revisit the fundamentals based on 2009-10 technical and data protection knowledge.
4) MS cannot use the DRD as justification to seek access to social networks which are outside its scope.

5) COM should analyse/evaluate the DRD as an exception to the right to privacy.

- Law enforcement relevance of data retention

1) Police authorities agree that the DRD is useful indeed but often lack precise statistics to assess the DRD's impact on their activities.
2) Statistics regarding the use of retained data are not always present.
3) A Public Private Partnership between LEAs and industry is necessary to improve the effectiveness of the DRD.
4) There is a lack of harmonisation of the period of and conditions for retention; moreover instruments to access data vary between MS.
5) Implementation of the DRD is ongoing; some challenges exist with regard to technologies (e.g. cloud computing, VoIP)

- Technological developments

1) It is too early to evaluate the implementation of the Directive: transposition was often delayed and the technical implementation continues to raise new questions.
2) Stakeholders must better work together in particular through forums to explain what industry needs to do and what LEAs can expect.
3) Prioritisation of issues is essential, e.g. by focusing first on what is reachable in the foreseeable future.
4) There are technological issues and challenges to be dealt with; they should not go beyond the scope of the Directive.
5) Down-to-earth cooperation is essential for the DRD to be used to its full extent while respecting its limits.

This second conference (the first one was on 14 March 2007) since the adoption of the DRD was chaired by Jacques VERRAES from Directorate F "Security" of the European Commission's DG Justice, Freedom, Security (DG JLS). Two Commission (COM) keynote speeches kicked off the meeting.

2. OPENING REMARKS AND PRESENTATIONS

Joachim NUNES DE ALMEIDA - Head of Unit, DG JLS, European Commission

Today all Member States (MS) should have transposed the Data Retention Directive. In sixteen months COM will present its evaluation of the DRD to the European Parliament and Council taking on board its impact on economic operators and consumers, the development of communications technology as well the statistics on the useage of data retained under the DRD that MS are obliged to provide in on a yearly basis.

After the last conference, an expert group with law enforcement, data protection and industry representatives was set up by the COM decision of 25 March 2008. It is a consultative group chaired by COM designed to facilitate the sharing of best practice regarding new technologies. It recently adopted it first position paper on SPAM e-mail, in

which it recommends that service providers should not be obliged to retain records of unsolicited bulk email ('spam') if it is filtered by the email provider and is never delivered to the recipient.

Key questions to address in the evaluation processes include: are the data retained under the (conditions set out in the) DRD efficient and relevant for law enforcement authorities to detect, investigate and prosecute serious crime and are the rights of citizens/end-users adequately and effectively protected. COM has seized the European Court of Justice (ECJ) to examine six cases where MS have not communicated national legislation implementing the DRD: NL, SE, IE, PL, AT and EL.

There is little statistical evidence that law enforcement authorities are at this moment using data retained regarding internet access, telephony or email to conduct law enforcement operations. Currently internet data is requested markedly less than fixed and mobile phone record data although this is likely to change and should be evaluated. The statistics show that the overwhelming majority of traffic data requested by police is under six months old, i.e. under the level that is set out in the DRD. COM calls on the 20 MS that did not make their statistics available (Article 10 of the DRD) for 2008 to do so quickly. If we cannot show the effectiveness of the DRD, there could be serious problems for other legislation in terms of access to information for police services.

Bernd LANGEHEINE - Director of Electronic Communications Policy from DG Information Society and Media (DG INFSO)

DG JLS and DG INFSO have worked together closely on the implementation of the DRD, including in the expert group. The upcoming evaluation will need to build on the expertise of both DGs. It is a very important Directive because it has far-reaching effects – it leads to seizable intrusions in the privacy of subscribers but it is an important instrument to let LEAs catch up with technological developments. It may also have a considerable impact on providers involved in its implementation.

MS who were waiting for an ECJ judgement before implementing the DRD have no excuse now as the judgement was delivered in February this year. The ECJ ruled that the legal basis of the DRD is correct.

A level playing field for providers of electronic services requires consistency and legal certainty, especially for those operating on an EU-wide scale. This is also very important for the evaluation of the DRD. It is important not to create distortions in competition.

MS have different approaches to cost reimbursement - from nothing to rather generous schemes covering capital and operating expenditure. Apart from reimbursement schemes, there are also other factors which determine the impact on economic operators, which need to be evaluated. These factors include the access procedures in MS, the response time required and the number of requests from LEAs.

Consumer confidence is a key factor for the information society, so that questions such as 'is there too much intrusion?' need to be analysed carefully. We need data from MS by early 2010 so that we have a good basis for the evaluation report, which is due in September. Mr Langeheine concluded by stating that we need to improve the perception of the DRD by the general public by making sure that it is useful, applied correctly and does not present an unacceptable threat to the privacy of citizens.

Peter HUSTINX - European Data Protection Supervisor

"Ensuring the Right Balance between Law Enforcement and Data Protection"[1]

We need to ensure the right balance between law enforcement needs and data protection requirements and to ensure the existence of effective protection in practice. The DRD and national legislation should meet conditions in Article 8 of the European Convention of Human Rights for a lawful restriction of the right to respect for a private life – that data retention should be done in accordance with the law (not just in terms of a formal legal basis but also in terms of meeting quality criteria such as clarity, precision, predictability and the existence of adequate safeguards against possible abuse), should be necessary in a democratic society for a legitimate purpose such as the prevention or repression of crime.

The relevance of the S. and Marper v. UK jurisprudence of December 2008 was highlighted. It is still an open question whether the DRD fully satisfies these requirements, given the political pressure under which it was adopted, the limited explanations in the preamble and the wide margins for implementation left to MS. This situation may give rise to court decisions, including possibly from both the ECJ and the ECtHR. Decisions of national courts on these issues are already in the pipeline.

Other key points:

- The evaluation of the DRD should throw light on the *necessity* and *effectiveness* of these measures. That means for instance that not only statistics on numbers of cases in which access was provided to retained data, but more substantive evidence will be required.

- There should be *adequate* and *effective* safeguards that retained data are *not* accessed or otherwise used for *other* purposes than those for which the obligation to retain these data was introduced.

- If the risks of security breaches or irregular or unlawful conduct are underestimated, there can be little doubt that both breaches and irregular conduct will happen in practice and that this will certainly undermine the legitimacy and credibility of data retention, also where it would be fully justified.

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-05-14_Brussels_data_retention_EN.pdf

Mr Hustinx expressed the hope that the Joint Investigation Action of the Article 29 Working Group about the way the DRD has been implemented in practice, which will include in-situ inspections, will contribute to the evaluation of the Directive.

Ruth ALLEN - Deputy Chief Executive UK Child Exploitation and Online Protection Centre (CEOP)

CEOP works with government authorities, police and other stakeholders to protect young people from paedophiles and sexual offenders, especially those who use the internet and other new technologies for the sexual exploitation of children.

Where crimes traditionally took place with the physical presence of two people, they are now being carried out online (e.g. online 'flashing' or grooming children on social networks for sexual abuse). Communications data is essential to the progress of investigations of these cases.

CEOP makes upwards of 10,000 individual requests for communications data annually (80% of them for internet data). Without this communications data, we cannot identify the offenders or victims. The DRD is a welcome initiative.

Given the complex nature of online sexual abuse investigations, the fact that many investigations cross national borders and that this takes time, the DRD is essential to ensure successful outcomes in this field. Currently, in the UK, communications service providers keep their internet data for varying amounts of time, from 30 days to two years. Given that there is no way of knowing which service provider we'll need to make a request to, this creates a lottery in terms of the success of an investigation. The results of a Croatian investigation into a website hacked to distribute indecent images of children showed that 40% of 5,236 IP addresses of UK suspects could not be investigated because of the data retention policies of service providers. This meant that potentially several hundred individuals with sexual interest in children could not be identified and remain unknown to LEAs.

The issue of data retrieval must also be addressed. It is unacceptable to have to wait several months while service providers retrieve data. To use communications data as a 'digital witness' of events online, it is essential that data is available to LEAs within a standard period of time after the event and easily retrievable in a timely manner to be able to support investigations. No lottery in data retention periods should be allowed to govern whether or not the victim of sexual abuse can be identified and rescued.

Simon KANG - Director, Technology Standards, Compliance & Security, UPC Broadband, Cable Europe

Mr Kang stated that the implementation of DR into providers' networks is both costly and complex.

There is uncertainty about implementation requirements with a lack of harmonisation across the EU for pan-European operators. Mr Kang stated that implementation guidelines are needed to support providers implement interoperable vendor solutions. Lack of technical guidance with regard to response times, the format for delivering data to LEAs, the retention obligations with regards to transit and third party providers, centralised storage, internet telephony services and unsuccessful calls to mention a few issues., results in diverging implementations across MS.

The assessment of Mr Kang is that the costs incurred by limited clarity are great and result in less investment.

The different reimbursement models across MS (e.g. the UK pays for capital and operational expenditure while some countries reimburse costs based on the amount of traffic passed back to the LEAs or per enquiry) results in unfair competition between pan-European providers.

The cost of the service to cable operators would come to around €2.5M (for fixed telephony data) just for capital expenditure with additional ongoing operational expenditure but depending on the size of the operator, it can be significantly higher. Mr Kang is of the opinion that for internet services the costs could be expected to be significantly higher.

This high cost to operators is met by a small percentage of government money allocated to fighting serious crime. Full cost reimbursement to operators is needed so that they can build and operate effective services for the law enforcement agencies.

Providers' systems were built to be business-grade rather than forensic-grade, designed to retain data for billing; making it suitable for LEA investigations requires significant adaptation and expense.

Mr Kang recommends developing an investment-friendly roadmap to reassure the market, and that would require a well-considered financial and technical impact assessment.

On-going measurements are needed to monitor the effectiveness of DR for law enforcement investigations.

Patrick BREYER - German Working Group on Data Retention

This German Working Group on Data Retention has filed a constitutional complaint (supported by 34,000 people) in DE against the DRD. His key points were that, because of the DRD:

- The prices of telecoms will be higher - the high costs incurred by providers are passed on to consumers or, if governments reimburse providers, consumers will pay more as taxpayers
- There will be less choice and fewer companies – small service providers have had to close because they could not carry the high fixed costs imposed by the DRD
- There will be less liberty – if people's use of email or their mobile phone is monitored then they will refrain from using it in certain situations
- Examples of people being reluctant to use their phones includes for contact with doctors, psychotherapists or drug counsellors

In a poll of 1,000 Germans done on 27-28 May 2008, the majority said that they would refrain from contacting martial crisis lines, drugs counsellors or psychotherapists via telecommunications, one in thirteen said that they had refrained from using their phone because of the DRD and every other person polled considered the DRD a disproportionate and unnecessary interference with their liberties.

In one incident, Deutsche Telekom had been found to have spied on employees and trade unions, something which shook the trust of consumers, while in another, TMobil lost customer data or had data stolen. Apart from its effects on consumer confidence, the DRA is also an obstacle to online business.

There is no proof that crime rates vary in a country according to whether the DRD is in place or that implementing the DRD has any effect on safety levels or reduces the number of children abused. The outcome of the DRD has been a disaster. COM should propose withdrawing it before the ECJ has to annul it for violating human rights.

Malcolm HUTTY - Director, European Association of European Internet Services Providers Associations (EuroISPA)

Full cost recovery for the service provider across the EU is needed so that the service provider can provide a better service to the LEA. This system would be fair and reasonable and would avoid distortions in the European telecoms market. There are significant capital and operating costs for the service provider. The initial systems design requires that operators do a comprehensive analysis of existing systems and extend that if necessary. The key capital costs:

- Initial system design
- Capital cost of collection and storage equipment
- Integration costs of integrating these systems into the existing system
- A search and retrieval system (to deliver data to LEAs in the form that they need it in and in a timely manner)

Operating costs:

- Access procedures and security surrounding that (e.g. you need to be able to distinguish a police officer from someone impersonating a police officer)

- Staff who implement the DRD (including training costs) and liaise with law enforcement
- Maintenance/updating of the system
- Continuing integration (e.g. to make sure network improvements don't inadvertently result in partial or total loss of retention capability)

There are three reasons EuroISPA believes services providers should be able to recover the full costs of DRD requirements:

- To enable investment in a quality service for law enforcement
- To remove market distortions created by the DRD
- To place service providers on an equal footing with other suppliers to law enforcement

Cost recovery enables investment by service providers in the systems that support law enforcement needs. Without investment, compliance is a pure cost centre so service providers look at what the laws require of them rather than anything beyond that. With cost recovery there can be a partnership approach that enables a quality, up-to-date service. This will meet law enforcement requirements more closely than legislation alone could ever achieve.

Currently there are differing retention requirements in different MS (e.g. different retention periods). Additionally, some MS reimburse capital expenditure, some operational expenditure. These differences create market distortions, both between providers in a single MS and within the European market. Relying exclusively on reimbursing operational expenditure through per-access fees can distort the market in favour of providers with a high volume of access requests. Conversely, relying exclusively on capital reimbursement can distort the market in favour of providers with a low volume of access requests. True cost recovery would remove the distortions in the market. EuroISPA wants a pan-European cost recovery regime (both capital and operating costs).

Cost recovery would also remove the market distortion introduced between the telecommunications sector and other sectors that supply law enforcement (from software to cleaning services). As has been shown, DRD creates a need to design, deploy and maintain dedicated systems specifically created to meet law enforcement needs. When other sectors (such as cleaning services or clothing manufacturers) deliver products or provide services to law enforcement authorities this is done at public expense. The same principle should apply in telecommunications.

For these reasons EuroISPA believes full cost recovery for DRD should be a legal requirement on MS.

Hakan HJELMESTAM - Information Security Manager, TeliaSonera, Stockholm)

Mr Hjelmestam represents GSM Association Europe in COM's Data Retention Expert Group. The expert group, called the 'Platform on electronic data retention for the

investigation, detection and prosecution of serious crime', was formally established in November 2008. It is looking into defining terms in the DRD, the technical, business and legal aspects of telecoms services (including roles and responsibilities) and producing guidance for MS. Encouraging sharing of information and experience it will promote input to and give help in the evaluation of the DRD. One of the areas it is working on is Voice Over Internet Protocol (VoIP), which is taking over from traditional telephony services. The group also sees the need for further discussion about the DRD and unsuccessful call attempts.

Thierry LE GALLOUDEC (French judicial police's central office for the fight against ICT crime)

Commander Le Galloudec underlines the importance of the DRD to fight crime, and states that there are no real problems with transposition apart from technical and legal issues. The main problems are anonymous services such as hotspots, and the location of the database where data are stored and that of the company which holds the data. Telecoms operators established elsewhere do not have the instruments to determine if they have the right to give location or traffic data to LEAs in France. This is a serious problem which France is working on. If the company is not legally represented in France it may say that it cannot provide the data. In that case police need a rogatory letter issued to the jurisdiction where the company is legally located.

In terms of costs, the French judicial police has worked with operators to create a reference document. They coded all the requests that police officers may make. An estimate was made on their price and the police refunds the cost based on a reference code. It is useful because investigators can estimate the costs of requests and operators can recover their costs.

Traditional operators managing networks are perceived to respect their legal obligations. Small companies however are more difficult to work with because they may not know that they are electronic operators in the sense of the law and have to fulfil the same obligations as larger operators. Need exists to explain the legal obligations to service providers.

Thomas ARNOLDI Federal Ministry of Justice, DE

Data can only be retained for six months in DE. DE transposed the DRD for fixed and mobile telephony on 1 January 2008 and for internet/email on 1 January 2009. The data retention obligation also applies to providers of anonymisation services.

There have been constitutional claims regarding transposition. The Federal Court has issued four temporary decisions but service providers must still retain data. The decisions cover the use of the data retrieved and a final decision is pending.

Data is only passed to LEAs if the crime is serious (i.e. would lead to a sentence of at least five years).

There have been complaints to the administrative courts by service providers, especially regarding the cost of the DRD. The government does not intend to reimburse the investment costs of service providers but to provide appropriate compensation for the retention and communication of data to LEAs.

According to statistics for a 10-month period (1 May 2008 to 28 February 2009), 12,742 judicial orders to retain data were issued. Data was retained in a total of 6,391 cases. There are some six million investigations in DE every year. So it is unacceptable that the media suggest that the DRD is excessive as we are talking about a small number of investigations. In 323 investigations, the data could not be provided. There were 175 investigations that could not be concluded because the data could not be provided. Very often data retention is the only way to solve a case.

Bob STAP (Ministry of Justice, NL)

NL is in the process of implementing the DRD. Members of Parliament were concerned about the impact of the obligations on privacy, the burden of costs on the telecoms industry and the disclosure of business information. A national law implementing the DRD will hopefully be adopted at the end of June.

During the negotiations, research by Erasmus University showed that the need for a certain period of data retention differs for particular types of crime:

- Normal crime – three months will be enough in general
- Serious crime – a period of one year could be justified
- Cold case – an even longer period could be justified

In its draft legislation, the NL government chose the period of 18 months for telephony and internet data. The Ministry of Justice stated that 18 months should not be understood as needed for all investigations but for serious crimes that lasted a long time and shocked society. In June 2008, the Second Chamber accepted the law on the condition that the period was 12 months for internet and telephony.
The Senate had serious doubts about the implementation of the DRD as each internet service provider (ISP) might choose a different system of storage and stressed the need for uniform agreements between law enforcement authorities and ISPs. Another important aspect is that the list of data to be retained is applicable on both service providers and network providers. There needs to be an arrangement between the service and network providers as to who is retaining the data and this need to be communicated to LEAs to avoid confusion.

Another issue is that there are a lot of small ISPs and a potential problem of their going bankrupt under the impact of the data retention obligations incumbent on them. The

Dutch government is trying to take into account the size of ISPs and offering them solutions in line with their importance.

3. METHODOLOGY FOR EVALUATION OF THE DRD

Prof. Elspeth GUILD – Univ. of Nijmegen, senior research fellow at the think tank CEPS

Too narrow a scope for the evaluation of the DRD can be considered as not useful as the central issues would not be touched on.

The evaluation needs to be based on three pillars:
1) Efficiency – how far and to what extent does the DRD fulfil its objectives?
Ms Guild referred to the remark by Mr Breyer who pointed to some worrying indicators of the consequences of the DRD for civil society. It will be a challenge just to get to the heart of the efficiency argument.

2) Legitimacy
Failing transposition in six member states is not a very good result by comparison with directives in other areas and hampers the evolution of data retention. Account needs to be taken of concerns in parliaments and civil society. It is not self-evident that parliaments accept the foundations of the DRD as correctly formulated.

3) Legality
Since the adoption of the DRD, there have been legal challenges – this should be fundamental to the assessment of the DRD. For example, a German court has made a referral to the ECJ (preliminary ruling) on the core legality of the DRD. It would seem unwise for COM to publish an evaluation of a DRD when the ECJ is considering if the DRD itself is fundamentally flawed.

Ms Guild pointed at the relevance of the Marper jurisprudent of the ECtHR of 4 December 2008 that postdates the adoption of the DRD so the reasoning was not available when the DRD was adopted. The decision applies in the EU and failure to take account of it in EU law would create a constitutional challenge in the EU because courts are required to apply the European Convention on Human Rights. There is a potential problem of hierarchy and coherence between EU law and the ECHR.

It is essential, as much as it is for phone tapping and covert intelligence gathering, to have clear, detailed rules on the scope and application of data retention measures. There is for instance no definition of 'competent authorities' in the DRD, which challenges the necessary clarity.

There must be minimum safeguards regarding storage of data, access by third parties and time that data is kept. These are different in different MS.

There need to be procedures for the destruction of the data. This acts as a guarantee against abuse and arbitrariness.

Martin WILLCOX - Director of Product & Solutions Marketing (EMEA), TERADATA

Mr Willcox confirmed that complying with the DRD is not cheap: although the unit price of computer storage has reduced significantly and vendors such as Teradata have introduced new product lines to store detailed data more cost-effectively, significant investments are still needed. In addition, large information systems attract significant additional costs in respect of design, development, operations and maintenance. These costs increase where there is a requirement for timely access to the data.

Mr Willcox stated that retention of traditional, circuit-switched telephony data is relatively uncontroversial, as consumers have largely embraced the idea of differential pricing and understand and accept the requirement this creates on Communication Service Providers (CSPs) to store usage data. Retention of IP data however is much more controversial: because this data is by nature more intrusive and also because the retention of this data does not create any direct value for the citizen. He stated that some ambiguity exists over the question of exactly who should capture certain types of IP-based communications data (e.g. the social networking site owner or the CSP that provides access). In addition, the inherent anonymity of some new, IP-based communication mechanisms create a challenge for CSPs and for LEAs.

Where telephony data is concerned the trend is for the capture of more (detailed) data to support legitimate business objectives (e.g. to store "billed call detail records" not just to bill the customer, but to support analysis of customer behaviour and trends in profitability, or to capture lower-level data to understand the impact of network failures on their best customers) The same trend is likely to play out where IP data are concerned.

Critical success factors for data retention are timely access (ability to directly access data and rapidly trawl through large data volumes), the capability of "scaling out" to gracefully accommodate ever-increasing volumes of data, and 'multi-temperature' data management (rapid access to the most frequently accessed "hot" data (typically the newer data) whilst permitting combination with older, "cooler" data to support more complex investigations). The advantage is that "cooler" data can be stored on cheaper storage devices, at the cost of some degradation in access performance. With increasing volumes of IP traffic, multi-temperature approaches will become more important, in combination with the relative absence, as yet, for CSPs to re-use this data to business advantage.

Mr Willcox admonished legislators to bear in mind that LEAs will increasingly have to re-assemble large and complex data-sets from several CSPs to resolve links between suspects e.g.: if A calls B using CSP 1, B sends an SMS to C using CSP 2 and C sends an e-mail to D using CSP 3, the relation A - D must be established). Binding EU-wide

standards would be necessary to support the integration and reconciliation of data reassembled on an ad-hoc basis from a number of communications providers.

The ability to re-use data and thus to create commercial value for CSP, is important to motivate the decision to invest in dedicated systems that improve service levels to LEAs. Failing this, telephony CSPs, for example, may choose to address the requirements of the Directive by 'just' deploying extended and enhanced existing commercial databases.

4. SEMINAR 1 - DATA PROTECTION AND PRIVACY ISSUES

Gus HOSEIN - Fellow at Privacy International described the 2005 political agreement on the DRD as having resulted in "a mess" and being very difficult to transpose into national law and apply in practice.

Issues raised:

- Do governments and LEAs have the right of access over all transactional information of citizens in MS?
- How sensitive is this information? argued that traffic data gives more information about an individual than DNA would.
- Mr Hosein stated that assurances had been given that access to retained data would be for those who were guilty, but this does not always seem to be the case. - Mr Hosein wanted to know how many innocent people's data was accessed

Parliamentary reports into the state of surveillance in society (e.g. in UK, NL & SE) need to be reflected in the new political settlement (evaluation of the DRD).

Mr Hosein asked how foreign web servers and social networking websites should be dealt with as this would be about ISPs collecting data that they do not have at present. Such an obligation would require a completely new political settlement.

Mr Hosein recommended considering the following issues for the review of the DRD:

- be explicit about the political settlement in 2005, especially regarding the collection of data.
- consider the impact of the December 2008 S. and Marper v. UK jurisprudence.
- be honest in political debates about the issues at stake: the DRD is about more than just 'who is calling who' (e.g. it is about location data too).

Hielke HIJMANS - European Data Protection Supervisor Legal Officer, argued that the DRD had not taken into account the need for effective protection for citizens. Effective protection for citizens where personal data is retained should be an important parameter for the evaluation of the DRD. Four key points:

1) Which providers does the DRD apply to? – Article 1 says "service providers" and "network providers" but it is not so simple in practice as they provide lots of different services (e.g. webmail or third party networks). It is not so clear who the LEA can go to, who looks after the safeguards for data protection or who is responsible for storage (the provider who is in direct contact with the customer or the network provider?).
2) Centralised storage – problems related to when a company is established in one country but stores data elsewhere (storage periods are different in different MS and companies must take into account the applicable law, which is difficult because there is no full harmonisation across the EU)
3) Applicable law - the DRD refers to data fully under the jurisdiction of where the data is generated whereas the Data Protection Directive has a different concept and it is not clear which law applies – the law of the country where the communication takes place or the country where the provider is established. For providers where the data is outside the EU, Mr Hijmans asked who has to retain the data then.
4) Security measures – Mr Hijmans pointed out that parts of the Data Protection Directive had been copied here (e.g. access only to specialised authorised personnel and an obligation to destroy data at the end of the retention period). Mr Hijmans described the latter as not really a security measure and questioned whether this was enough in a complex environment.

Under Article 4 of the DRD, Mr Hijmans noted that access to data was only given to authorities in specific cases and that it could not be accessed by everyone (e.g. for data mining or profiling). National law must implement the DRD. This should be an important part of the evaluation. COM should look at what the national law says about access. The evaluation should ensure that there is effective protection for citizens in the revised DRD.

Erik JOSEFSSON[2] - Privacy activist and European Parliament candidate for the Swedish left party, said that the DRD had been adopted in too much of a rush.

At the time of the adoption of the DRD, the copyright industry had not added clarity to what was already a complex directive by arguing for amendments to increase retention times and open up data use for their business models to fight piracy with the data retained.

There was a great deal of controversy surrounding the DRD when it was discussed by the European Parliament and some MEPs expressed "indignation, anger and frustration" at the way in which negotiations had been carried out between the chairmen of the big political groups and the UK presidency of the EU at the time.

The issue of data retention has been a factor contributing to the formation of the Pirate Party (now SE's third largest party with a big youth following), a one-issue party focussing on intellectual property, freedom of knowledge and protection of privacy.

---

2 http://www.erikjosefsson.eu/sites/default/files/Erik_Josefsson_DRD_presentation_20090514.pdf

Mr Josefsson's policy recommendation is that Sweden should resist to transpose the DRD and that Commission should refer the non-communication by Sweden to the ECJ aiming at partial annulment of the DRD, namely the part concerning the internet data.

Achim KLABUNDE – European Commission DG INFSO

The DRD applies only to electronic communications services. Information society services such as webmail, social networking sites, search engines, e-commerce sites and online games are not covered by the E-Privacy Directive or the DRD. MS must address such services with other legal bases and take into account the Data Protection Directive too.

There are safeguards built into the DRD. The article on access to data stipulates that it is for competent authorities only in specific cases according to procedures defined by national law. The limitation to 'specific cases' and the requirement of a 'procedure defined by law' underline the principles of a democratic society. The explicit obligation to destroy data at the end of the retention period is a good protection against misuse, and a very clear data protection provision.

The Directive also refers explicitly to the necessary security measures, which need to go beyond business grade security to forensic security (i.e. the data must be secured as potential evidence in a court case) because, for example, large-scale organised crime might be trying to access and destroy data.

Another safeguard is that the evaluation is being done (2010) in a short period following the adoption of the DRD (2005) and three-year transposition period for MS.

The DRD has had many effects, e.g. the economic impacts on the sector might go beyond what was expected at the time. How the safeguards in the DRD actually work should be verified in the evaluation.

Open discussion

Mr Josefsson said that we need to learn to use technology to fight crime and suggested starting again with a dialogue between the technology (but not business interests) and law enforcement communities.

Mr Hosein said that many countries (e.g. Canada and the US) get by without a data retention directive and the EU could have alternative legal measures instead of the DRD.

Andrew Knight (UK Home Office) said that the UK has used the DRD to disrupt a number of terrorist operations and could not have done that without it. Mr Knight warned

against comparing the strong European data protection regime with other countries' regimes.

Mr Hosein said that there is a good case for targeted recording of transactions but keeping a history of transactions for everyone was a case that still had to be fought.

Mr Knight (UK Home Office) said that 524,000 pieces of communications data had been accessed. At the time that they are accused, a majority of those are innocent, as people are regarded as 'innocent until proven guilty'. The UK tries to ensure that, when someone is accused, data are also used to prove they are not related to the crime. This is part of the consideration of necessity and proportionality, and functions as a built-in safeguard. Personnel is fully trained, there is a full audit trail (of the person on the frontline, who signed the request off and what data they got back) plus an independent oversight officer (a member of the judiciary) who looks at the data after the event and judges retrospectively if the decision was necessary and appropriate.

Mr Hosein was not convinced.

5. SEMINAR 1 – SUMMARY BY CHAIR Prof. ELSPETH GUILD

1) Effective protection is not yet fully in place in terms of storage (what law applies to protect individuals), what security measures are applicable for retention of data and who has access and in what circumstances.
2) There is a lack of knowledge about the impact of implementation on companies and individuals and there has been questionable democratic legitimacy.
3) There is a need to revisit the fundamentals based on 2009-10 technical knowledge and data protection knowledge.
4) MS cannot use this DRD as justification to seek access to social networks as this is outside its scope and would need to justify that via the Data Protection Directive.
5) COM should analyse/evaluate the DRD as an exception to the right to privacy (in line with ECJ case law on public security in the free market).

Asked whether prosecutors should destroy data at the end of the retention period or if they could store it, Ms Guild said that this is a problem of different systems of law and the point at which 'data' becomes 'evidence'. In the EU, we have an incomplete set of rules in judicial cooperation in criminal matters and an uneven application of the European Evidence Warrant. If the retained data is used in court cases, the normal legal rules of MS apply.

6. SEMINAR 2 – LAW ENFORCEMENT RELEVANCE OF DATA RETENTION

Kurt ALAVAARA - National Police Board, Stockholm, SE

SE did not yet adopt legislation for data retention but intends to present a bill before the summer that should enter into force by 1 January 2010. SE has regulations for access to the data that are kept by service- and network providers for their own purpose. (Handover of the data can be done either electronically or semi-electronically, e.g. CDs, DVDs).

Communications data is essential for the investigation of serious crimes.

The importance of the protection of the data from unlawful access was stressed. The encryption of data and limitation of access when there is a legal requirement was qualified as an interesting development.

The need exists to follow up on the trend which is moving from traditional telephony to IP-based telephony. To keep abreast of developments in the realm of IP services and cloud computing, public authorities need close cooperation with industry to ensure that law enforcement, data protection and privacy needs are met.

The challenge is bigger if data is kept outside the EU. What rules are there to protect these data and how can it be handed to EU LEAs? How long the data is stored if it is stored elsewhere and how it is protected from unlawful access? These issues depend on the law in the relevant jurisdiction.

The DRD does not cover all internet services (e.g. chat or FTP) but it is very important for LEAs to also follow this as there is concern that these services are used by terrorists and criminals to avoid detection.

Asked to assess the added value of the DRD, Mr Alavaara mentioned as an example that currently mobile phone providers do not hand in incoming call information any more as they don't need it for billing purposes and so don't store it. In terms of storage time, he mentioned that this varies enormously: sometimes data is needed a couple of hours after a crime occurred or six months afterwards or over a year later or ten years later.

Asked if it is possible to do local interception to catch 'web chat' live, Mr Alavaara said that the DRD does not cover chat or FTP but it might be possible to take care of interception if the telecoms address is known.

Asked about how small operators were dealt with, Mr Alavaara said that the current national data retention proposal (under discussion) covers all service and network providers. They are all obliged to retain communications data irrespective of their size but the postal and telecoms agency can give exceptions. Furthermore, small service providers also have a possibility to outsource retention to keep costs down.

Asked about access to data to prevent crime, Mr Alavaara said that at this moment law enforcement authorities in Sweden don't have access for prevention but an inquiry is going on suggesting that they do.

Ludek HAVLICEK - CZ police, Prague

CZ in fact implemented 90% of the DRD in 2005 as it was already in the process of passing a relevant law at the time. Telephone, internet and voicemail data must be retained for six months. Internet also covers FTP, chat and web pages. Mr Havlicek regretted that after implementing the DRD, CZ would lose these data. From a law enforcement perspective this is not desirable as these data are important in investigations and prosecutions.

In cases of a suspicion of a serious crime, the police can access retained data based on a court order, but in cases of e.g. terrorism it can directly go to an operator on the basis of the Police Act. The input (request) and output (reply) are standardized which facilitates communication between police and providers that know how to answer and provides police with good data.

On the basis of the available 2008 statistics, CZ has made the most requests in the whole of the EU:

- Fixed: 4,000 requests per annum
- Mobile: 98,000 requests per annum
- Internet: 800 requests per annum

Most requests are made in the first three months from the retention of the data. This does not mean however that data is not necessarily unimportant after six or nine months. Law enforcement authorities would like to extend the national retention period to nine months but Mr Havlicek doubted that this would happen.

Other points:

- Fixed telephony requests are going down as people are not using fixed phones that much any more
- There is a growing number of requests for mobile phone data
- There is a huge growth in the number of requests for internet data because of the development of the internet market
- The data are very important for investigations

Charles MILLER - UK Home Office

Before the DRD, the UK had a voluntary retention regime which dates back to post 9/11. The issue for the UK in its funding model based on law enforcement requirements is about the retention and also the retrieval of data by the service provider.

The UK pays for the retention of data, the retrieval system in the service provider and, in addition, every time there is a request to make data retention cost-neutral to the service provider. However, even though the UK Government pays the service provider to retain their data and build a retrieval capability, and law enforcement pays to maintain that capability, there is a still a problem in that such projects are viewed by senior members within service providers as simply 'non-profit making' and therefore not a priority in the company. It is therefore essential to make sure that there is engagement at a very senior level within service provider to ensure that those members are aware of their legal obligations and the availability of UK Government money to assist with compliance i.e. retention AND retrieval capability that is fit for purpose.

The communications data is an unintended witness of the digital movements of terrorists, other criminals and witnesses alike. It is significant to identifying other evidence. It can help police establish the location of suspects from their mobile phone so that they can recover other evidence such as relevant CCTV, DNA, travel documents etc. The analysis of the data can reveal that the criminals may have stopped communicating e.g. a data gap can be significant too as two conspirators may have stopped communicating by phone because they are meeting face to face. Communications data gives a timeline and an investigative hook.

Data protection lobbyists may say that data retention is pointless as criminals can circumvent it (e.g by SIM card swapping) but criminals make “mistakes” such as leaving their mobile registered in their name or leaving their home phone number within it.

A report by the Crown Prosecution Service concluded that often information from communications data convinces defendants to plead guilty, especially in conspiracy cases. Without the DRD, the report says that 70% of serious crime offenders would have been acquitted or simply not prosecuted.

Stefano ZIREDDU - Postal and Communications Police, Italy

Italy has implemented the DRD and has a lot of experience of using retained data in criminal investigations, in particular those regarding domestic terrorism and the mafia.

Data retention was introduced into Italian law in the early eighties and was very useful during the investigations in the context of the assassination of Judge Falcone. Italian investigators could retrieve data from five years before, which was useful for ongoing investigations. The parliament reduced that to four years and then a privacy code reduced it to six months in 2002-2003. This was a huge problem in Italy as it made it very difficult to face the mafia with only six months of data. Fortunately the DRD came along and allowed Italy to change the system.

Mr Zireddu stated that, from the point of view of a specialised investigator of ICT crime, the absence of data incapacitates the conduct of an investigation. Retained data has been important in various cases, including an investigation of an Imam in Perugia who was looking for recruits to send to Iraq to be kamikazes.

In Italian legislation only the judiciary, and not the police, can order an ISP to show retained data. Police must request the prosecutor to ask an investigating judge to order the telephony or internet operator to provider certain data. It is the only way to receive retained data concerning persons or suspects under investigation. By and large, after having applied the national legislation transposing the DRD, Italy is satisfied with the DRD.

Mr Zireddu mentioned that, in Italy, many meetings took place between police and operators about "unequivocal IPs", which concerned the problem of associating an IP address with a single person. In practice, during an investigation, the police have to target the machine (computer) first and then the person behind it.

In Italy, internet access data must be retained for 12 months and phone data for 24 months. Mr Zireddu expresses the hope that the legislation will provide the same retention period for telephony and internet.

Asked about VoIP, Mr Zireddu said that this is a problem for Europe and the whole world and not only Italy. Skype is a big problem that must be solved by speaking with providers. At the moment Italy has proposed that the EU discuss this theme. The problem lies more in the willingness to solve it than the technical side of things.

Asked how information is transferred from telecom providers to police forces, the speaker said that different operators are present now on a portal where police can ask for the name of the customer, the phone number and the number of lines. A portal for sending requests for live data (interception/streaming) is missing but law enforcement authorities are discussing this issue with providers and expect to arrive at a solution by the end of the year. The data available via the portal is data that a customer gives when (s)he subscribes to a mobile phone contract (e.g. identification of customer, residence, date of birth etc.).

To get access to data held by a provider, the LEA addresses a request to the portal and obtains an answer within a time range of a quarter of an hour to half a day. This does not apply to live information of phone calls on the portal because that has not yet been implemented. Telecom Italia and Vodafone have portals. Some providers do not have such a facility. Lawful interception is only used in the context of criminal investigations.

Mr Ilmari VIRO, National Bureau of Investigation, FI

The DRD provides for a minimum set of standards. Extending the data to be retained would, according to Mr Viro, be meaningful but possible only if political consensus exists. The period of retention is 12 months in FI.

Implementation obliges the operators to retain the data. FI reimburses capital expenditure and operational expenditure. Its law enforcement authorities are restrained by a limited budget. Mr Viro stated that it should be up to LEAs to decide which operators to ask first

and how much information to have – e.g. ask the biggest operators first before turning to the smallest ones. The DRD would not allow such differentiation.

To include retention of data of Skype (or similar) based communications, it would be necessary to enact a directive concerning application service providers that should be obliged to change their business model. Otherwise it would be impossible to obtain such data.

7. SEMINAR 2 - SUMMARY BY CHAIR Mr GWENDAL LEGRAND

1) All police authorities agreed that the DRD is useful for their work but do not always have precise statistics to assess the DRD's impact on police work. A UK study showed that 70% of data collected had been used.
2) Not all countries can give precise statistics regarding the use of retained data and its impact on law enforcement activities. UK analysis/data mining tools have been put in place to allow data from e-communications systems to be compared with surveillance data.
3) A partnership is needed between LEAs and industry to make the DRD effective (e.g. portals in Italy giving police access to data from some of the bigger operators).
4) There is a lack of harmonisation. Means of access to the data varies. In some cases, police has direct access while in others police have to go via a judge. Where the DRD has been implemented, police do use the data.
5) Implementation of the DRD is ongoing; some problems exist with regard to new technological solutions on the net (e.g. 'cloud computing', Skype). There may be problems of adaptation implementing the DRD with regard to these new technologies.

Asked if there is one standard for operators on how data should be handed over to LEAs, Mr LeGrand said that there is a lack of standardisation (e.g. sometimes portals and sometimes not). For there to be an effective use of data, common standards for interaction between authorities and operators is necessary. The security of the data transferred (data quality) is important too. A common data collection format would be very useful, leaving open the question of security of transfer and monitoring, and the identification of officials requiring the data.

8. SEMINAR 3 – TECHNOLOGICAL DEVELOPMENTS AND CHALLENGES

Philippe GERARD - deputy head of unit, European Commission, DG INFSO B3 in introducing the workshop warned that not all possible developments might be covered by the scope of the Data Retention Directive. After having heard the law enforcement side

regarding challenges, the floor was given to the operators who must implement the DRD in practice, and finally to one provider of security software and hardware solutions. .

Pertti SOVELIUS - Detective Sergeant at the National Bureau of Investigation, FI

Mr Sovelius produced a 'traffic light system' to point to where the main problems encountered in applying the DRD.

Green - Mr Sovelius has no problems with the DRD and encourages cooperation between LEAs and private companies to develop a data retention and retrieval system as we need tools such as this to fight cross-border crime.

Yellow – We should focus on 'stable' techniques that already exist and not follow every new gadget coming onto the market. The DRD works pretty well from a technical point of view.

Red – True functionality depends on MS' technical implementation. If this is done in a short-sighted way, then we will have problems. FI has a cost coverage system for what data operators must retain and store. The Finnish state pays all the costs. If there is a change in business model, what do we do? Pay again? This is a big problem to solve.

As for future challenges, Mr Sovelius asked how we could keep up with new technologies, what the operational limitations of retrieval systems were and how data could be handed over to other MS without unnecessary delays.

In the future, we must think about how to take the DRD into account before building a system. Mr Sovelius raised the issue of what to do with some technologies such as Messenger, which do not fall within the scope of the DRD.

If a service provider operates in MS jurisdiction then the LEAs should not have to file letters of request. Mr Sovelius gave a hypothetical example where the Finnish authorities may want to wiretap communication but the operator says that all the servers are in SE and that the authorities would need to send letters of request. His view is that it should not be this way and that the authorities must have the information from national channels if the service is offered on Finnish territory.

Yasmine OURARI - Legal Advisor to the Belgian Federal Judicial Police

Around 82% of emails are spam. There is too much data so filters need to be applied. Industry needs to reinforce its actions here, blocking spam, which can be the origin of fraud and viruses. Reducing spam reduces crime and can save police time. We can support the solution of the expert group regarding spam.

The DRD targets service providers. Webmail is an e-communication service so service providers are included. The text of the DRD does not exclude webmail explicitly.

Webmail data is crucial for investigations (85% of judicial requests for internet identification concern emails and 90% of these email requests are webmails). We believe that access to this data should be possible, without a rogatory letter, if the company has a legal office in the country even if the service is in another country.

Internet telephony is the biggest problem because there is no definition of it in the DRD. Skype, GoogleTalk, MSN all enable peer-to-peer dialogue. We need to identify what we see as internet telephony. In four to five years we expect it to be a more extended system and to replace the telephone system. People will no longer have a telephone number attributed to them at a physical address. We need to be able to identify the end user. People can put 'Mickey Mouse' but this is clearly false data. It is important to make an effort to identify the person.

Another important issue in Brussels is 'WiFi'. People can take their laptop somewhere and only need a login and password but there is no user identification, which gives users anonymity.

Mr Hutty (EuroISPA) said that is commonly understood that the telephony aspect of internet telephony refers to using PSTN numbers and excludes voice communications such as computer games.

Mr Sovelius warned that there would be 27 different MS definitions if we did not define internet telephony and that this needed to be dealt with.

A representative from the European Data Protection Supervisor's office pointed out that the DRD is not only focused on LEAs but also on the rights of data subjects. Mr Sovelius suggested a balanced instrument.

Ms Ourari said that it would be a problem if it did not cover the needs of LEAs.

Mr Hutty can understand why the chief of police sees the law enforcement needs but he also sees the data protection and human rights points. Regarding webmail, Mr Hutty said that while some web based messaging services may be covered by the DRD, others are information society services that are not in the remit of the DRD. Only Public Electronic Communications Services are covered by the DRD. EuroISPA seeks to cooperate with law enforcement needs but obeying the law must come first.
Gert WABEKE – national telecom provider KPN, NL said that KPN was struggling with implementation. The DRD was aimed essentially at telephony but has been 'copied' to the internet.

His points included:

- What kind of obligations do network and service providers have?
- Who is responsible for what kind of data?
- What is requested and how can it be disclosed?
- Performance requirements (expectations) with regard to the retrieval of information in combination with the availability of information after an event (i.e.

minutes necessary to make retained data available in the data retention domain after a telephone call or internet access event), risk going beyond business practice.

- What do we retain?

Mr Wabeke pointed out that we are in the process of learning concerning internet information. Which information is used by an operator for its business purpose and which data is requested for lawful investigation? How does an investigation use this information and is it useful? The complexity of internet and internet-related services is, in relation to telephony, not that straightforward and well-defined. It could be that someone does not know that his/her computer is being used for criminal purposes and that the real criminal activity is hidden via a number of computers in different countries. Mr Wabeke stressed the complexity of the subject.

Cost reimbursement is not the only issue of relevance to service providers. Others concern the provider's role in safeguarding the privacy of customers on the one hand and compliance with the law and lawful intrusion of privacy on the other hand. Both are linked in a complex balance. A comprehensive approach is required. The rules and obligations should be considered through the chain of provider and investigation within the boundaries of the regulatory and legal framework.

Asked how KPN (Netherlands) applies the DRD on a daily basis, especially with regard to the internet, Mr Wabeke said that, under the current law (since DRD has not yet been transposed in Dutch Law), KPN must retain data for three months but for telephony only. The current practice is focused on information about mobile telephony, fixed telephony and telephony over the internet. Internet-related information requests are developing at a slow pace and represent a very small percentage of requests.

Robert MOL - Principal Marketing Manager, Symantec EMEA

Some 35 to 60 billion emails are sent worldwide per day. The amount of new technological information produced is doubling every year. The question is how to deal with that data. The growth in information has led to more infrastructure complexity. The number one concern is how to deal with infrastructure complexity and the DRD and other legislation and how to make the infrastructure flexible enough to cope. Mr Mol stressed that the brand protection of a company is at stake and that there is a need to distinguish between data for the archiving (of less value) and data that you need to access and retrieve more speedily.

There needs to be a balance between how we manage infrastructure and the adoption of new technologies (e.g. ‘virtualisation’ – with data in a virtual environment that is not seen on the computer server).

There are two major challenges in terms of technical implementation:

1) Security is no longer just about virus and anti-spam protection but needs to be reviewed in a broader context including Data Loss Prevention, Device Control, Data Encryption and infrastructure management. 95% of vulnerabilities that a company faces are a result of a poor system of configuration and patch management. Only 5% of the vulnerabilities are actually to do with zero day attacks, viruses and other external risks.
2) Data centre management – increasing storage costs and low utilisation mean that a balance needs to be struck between having to store data for long term through archiving and low cost storage means such as tape, for example and having a flexible data protection model that allows secure storage and fast retrieval based on the needs of the business. This includes regulatory requirements.

If we consider that on average we store a data file (documents, etc.) seven times in different locations of the infrastructure, the need for accurate de-duplication to save storage capacity and optimise the retrieval process of data is another important factor in effective data centre management.

In the context of DRD it is important to factor in the need for organisations to protect their intellectual property from both internal as well as external threats. Protecting such information from unauthorized distribution and access is the number one priority for businesses. A holistic view of information protection is needed to ensure that DRD and other regulatory requirements are made part of the enterprise architecture and do not stand on their own.

Asked what could be done to improve the adoption of DRD by member states, Mr Mol said that "based on the presentations heard today, the implementation of DRD seems to be the subject that requires further investigation". His suggestion would be to consolidate the views of industry, ISPs and the telecoms business in a working group to establish guiding principles for the various technological aspects of adhering to the Directive.

Matthijs Dammers – Ministry of Economic Affairs, NL suggested focussing on what is working and not on new gadgets. The evaluation could be divided into an easier part covering telephony (showing that it is worth doing) and a more difficult part covering the internet, where more research is needed.

Patricia Brown (Home Office, UK) said that it should be relatively easy to evaluate the DRD on the telephony side as most countries have a lot of experience of that. It will be more complex for internet providers, especially the six countries where it has not been transposed. There is a steep learning curve regarding new and old technology. In the evaluation, it is not a simple 'yes or no' but we need a qualitative view regarding investigations, training etc.

Mr Hutty said that the starting point was that intrusions must be justified. Mr Hutty cannot see how you can conclude, if it is not used, that the DRD has been a success. Whether or not it has been implemented and whether public authorities used it must be central to the evaluation of the DRD.

Asked what they saw as the main issue on the application of the DRD, the speakers pointed to the retrieval of data **(Mr Sovelius)**, the issue of internet data and questions regarding the cost of implementation and which operators were affected **(Ms Ourari)**, standardisation work and clarifying responsibilities **(Mr Wabeke)** and understanding what exactly needs to be delivered and in what mode **(Mr Mol)**.

Gert Wabeke (KPN, NL) said that KPN (Dutch service provider) was struggling with the implementation. The DRD had been developed essentially aiming at telephony and intercepts but had been copied to the internet.

He addressed the obligations of network and service providers, their responsibilities for certain data, the requests made and the mechanisms of disclosure including for urgent requests, and the data that are retained. At this moment, the NL service provider is in the process of defining how internet information will be used, and is reflecting on the rules and obligations through the chain of providers/operators.

9. SEMINAR 3 - SUMMARY BY CHAIR Mr PHILIPPE GERARD

The objective of the workshop, as a contribution to kick-starting the process of evaluation of the Directive, was to identify current challenges to its implementation, in particular technology-related challenges.

1) It is too early to evaluate the implementation of the Directive: transposition was delayed in many quarters and the technical implementation on site continues to raise several issues.
2) Stakeholders must work together to improve implementation and find practical solutions for day-to-day cooperation. There needs to be more cooperation in relevant forums to make clear what industry needs to do and what LEAs can expect.
3) Prioritisation of issues is essential, perhaps by focusing first on what is reachable in the foreseeable future, leaving other issues for future review.
4) There are technological issues (e.g. webmail, VoIP) – and important challenges and work needs to be done here, but there are limits to the scope of the Directive which cannot be stretched.
5) Overall, down-to-earth cooperation would be essential for the DRD to be used to its full extent while respecting its limits.

Asked if it would be a good idea to organise platforms to deal with different pieces of work to solve some of the problems raised today, Mr Gerard said that such platform already exists and that more needed to be done to deal with basic questions such as which data needs to be retained, how can the data be passed to LEAs and what format is should be in.

10. CONCLUSIONS

Mr NUNES DE ALMEIDA – European Commission – DG JLS, recalled that the DRD came about as a political reaction to the London bombing attacks of 2005 but that its scope is not limited to fighting terrorism but also to tackle all forms of organised crime. At this moment, MS' security services say that the terrorist threat is as strong as it was a few years ago.

It is encouraging to note that the DRD is being used by many LEAs of MS but to give COM the relevant background to carry out the evaluation, MS need to give COM more convincing reasons showing the usefulness of the DRD in fighting organised crime and terrorism. National annual statistics are a very important source of information in that respect and MS were called upon to provide them according to the obligation in Article 10 DRD.

MS need to say why they need to use retain data without of course jeopardising national security in that process. It is important to convince those who are not convinced about the DRD as to why it is necessary and for that the ongoing help of the participants in this conference is needed.

Regarding the impact of technological evolutions on the validity of the data retention concept, this is a challenge to the legislator: legislation is potentially intrusive to civil liberties for which reason it needs to be as precise as possible but it should not be a straightjacket that would stifle technological evolution.

Jacques Verraes