Public hearing in Joint Cases C-239/12 and C-594/12 (9 July 2013)

Pleading of the EDPS

Mr. President, Members of the Court, Mr. Advocate General

We appreciate that, for the first time, the Court of Justice under Article 24 of its Statute has invited the EDPS to supply information in a case before it.

The Court has asked us to provide information on four specific questions.

Allow me to start with Question 3,which we consider of a more general nature. We note that in *Schecke and Eiffert* your Court assessed compatibility with Articles 7 and 8 of the Charter without systematically distinguishing between the two provisions. The present case shows however that a distinction is useful. The EDPS therefore would respectfully suggest that your Court should consider a double test under the Charter. As Articles 7 and 8 have a different nature, the separate requirements of both must be fulfilled.

Let me start with Article 7.

Article 7, which *grosso modo* corresponds with Article 8 of the Convention, can be seen as a "classic" fundamental right. It is a right that protects the individual primarily against interference by the State. In our view, and this is shared by most parties present today, the Data Retention Directive constitutes such interference to the right to privacy. I recall case law of the Strasbourg Court, in particular the case *Malone v. UK* (Application no. 8691/79), on the interception of communications and release of records of metering, and on telephone data in particular.The ECtHR has stated that "release of that information to the police without the consent of the subscriber also amounts [...] to an interference with Article 8 ECHR".

Interference requires justification. I will return to that briefly in a moment.

Article 8 formulates as a separate right the protection of personal data, that must be seen as a proactive right TO protection, that is NOT limited to protecting against interference by the State. Article 8 gives the individual a claim that his or her personal data can only be processed if

certain essential requirements are fulfilled. These essential requirements are laid down in Article 8 (2) and (3) of the Charter:

- First, there must be fair and lawful processing, for specified purposes

- Second, transparency must be ensured, by giving the data subject rights to access and rectification.

Third: there must be control by an independent authority.

These are the rules of the game which were based on existing laws on data protection. Interference by the State by legislative intervention may specify the rules of the game for data processing, and by doing so, interference may strengthen the protection.

In other words, whilst Article 7 protects the individual against interference by the State, Article 8 entitles the individual *ex ante* to protection according to certain standards whenever and by whomsoever his data are processed.

Let me now turn to the justification for the interference under Article 7. The EDPS has argued on several occasions that retention as foreseen by the Directive is not sufficiently justified. I refer in particular to our opinion of 2011 on the evaluation of the directive, which you can find on our website. In our opinion we made three main points :

- ◊ first, the necessity in a democratic society has not been sufficiently demonstrated.
- ◊ second, the adoption of the Directive at the beginning of 2006 was not preceded by a proper assessment of other, less intrusive means that do not require blanket retention of broad ranges of information about all EU citizens for up to 2 years.
- ◊ third, the directive lacks foreseeability, since - as this honourable Court stated in Joined Cases C-465/00 and C-138/01 and 139/01, Rundfunk - the law should be formulated with sufficient precision to enable individuals to adapt their behaviour accordingly. Specification of the provisions, in particular Article 4 of the Directive, is fully left to the Member States. This is simply not enough. The EU legislator should not adopt a legal instrument, that contains an interference with a fundamental right, without giving specification of the interference - by the State!- in the instrument itself. Also under Article 95 EC such specification could have been given.

I will now discuss the assessment under Article 8. The data subject must have the assurance that all the essential requirements of that provision are met:

- ◊ In the first place, the data retention directive does not sufficiently address the need for purpose limitation. We give your Court into consideration that the purpose of processing is not well defined in the Directive, since "serious crime" is not defined. Furthermore, there is the famous "loophole" with Article 15(1) of Directive 2002/58/EC which allows Member States to use the data for other, not foreseen purposes.

- ◊ In the second place, it does not provide for sufficient safeguards, enabling the data subject to invoke his rights to access and rectification, in particular with regard to the activities of the police. The situation is not clear when a citizen asks to be informed on requests made by national law enforcement authorities. It is even more complicated when the data are used by law enforcement authorities. How is it ensured that individuals can invoke their rights? These are important questions which should not have been left open.

Mr President, I now turn to the first question.

This question, in essence, addresses the effectiveness of the Data Retention Directive for the purpose of combating serious crime, because

it might be possible to use electronic means whilst avoiding that traces are retained under the directive.

Let me give you two examples:

- ◊ Firstly, criminals will use stolen pre-paid SIM-cards together with disposable handsets;
- ◊ Secondly, purely Web-based services relying on the Internet Protocol (IP) do not fall within the scope of the directive because they can not be considered "providers of publicly available electronic communications services or of public communications networks". However, they offer very similar functionalities, such as VoIP ("Voice over IP") telephony, instant messaging applications, social network messaging platforms, etc. All these services make it easy to disguise your real identity.

This brings me to a fundamental point: as already explained by other parties today, it is very difficult to communicate in a fully anonymous way. You have to use a sophisticated combination of the possibilities of these services and additional illegal means, such as stolen credit cards, and fake identities in order to make identification really very difficult. Only terrorists or individuals engaged in serious crime will have the means and the motivation to do this.

Data retention imposed by the Directive 2006/24 could thus have the perverse effect that criminal organisations will find a way to communicate anonymously, while the majority of law-abiding EU citizens find their communications data retained at a massive scale.

In reaction to the first question posed by your Court, we would respectfully advise the Court that there exist wide possibilities for circumvention of data retention under the directive; these should be taken into account when assessing the necessity and proportionality of the directive.

Mr. President, the second question posed by the Court addresses the issue of profiling of individuals, and thus points at specific, but potentially very intrusive consequences of the retention for individuals. We note in this context that:

- ◊ although traffic and location data do not include the content of a communication, they can be of an extremely sensitive nature, as I will explain shortly.
- ◊ the directive foresees the retention of these sensitive metadata of all 500 million + EU citizens

The Data Retention Directive, read in combination with Directive 2002/58, limits the use of the data by telecommunications providers, and does not allow for profiling by those providers. However:

- ◊ traffic and location data are of immense commercial value for the service providers retaining it and for other business entities,

and so:

- ◊ there is always a risk that the data are accessed or hacked by persons that are not authorized to use it, and
- ◊ there is always a risk that authorized persons use the data for non authorized activities.

Moreover, the Directive leaves a broad discretion as to the access and use of the data by law enforcement authorities. In this context, we should not forget the legal loophole allowing Member States to use - under Article 15 of Directive 2002/58 - the data, outside the scope of Article 4 of the Data Retention Directive. This is even more important in view of progressing technologies, in what we call now the world of 'big data'.

This leads to the issue of profiling:

- ◊ Access and use of data may be clearly limited in principle.

- ◊ However, in practice technology now allows the identity of a person to be determined over time, by using location data. Location trails, as they are created by the retention of data under the Directive, are highly unique, and they also provide detailed insight into the habits and life of the individual.

- ◊ In addition, the communications themselves, whether fixed or mobile, place each user in a network of social and business relationships, and allows contacts to be identified.

- ◊ Furthermore, an important objective of retention of telecommunications data *by government* is traffic analysis. This is an old concept which can be understood as inferring important information from patterns in communications.

Finally, we should not forget that the retention also covers the increasing number of smartphone applications which communicate automatically, without intervention by the user. Smart phones run many applications which establish communications for their functioning, for example, to update weather information or stock prices, load emails, and find the best route to a new place, as well as an ever growing range of other services. This is an on-going

development, and it is significantly increasing the degree of profiling possible on the basis of retained data.

It is against this background that the EDPS answers the second question of this Court: The Directive certainly increases the possibilities to create and use personal profiles, whether legally or illegally.

I will now turn to Question 5 (b), on security and outsourcing.

Security is of crucial importance to personal data protection as it ensures respect for all the other safeguards provided for by primary or secondary law. The EU data protection directives therefore require security measures, in generic legislative provisions. However the data retention directive should have, but does NOT specify these generic provisions; Article 7 of the directive basically repeats the provisions of Directives 95/46 and 2002/58. We feel that such specifications are especially required in the present case, in view of the risks presented by the massive scale of data retention. I mentioned those risks before, but would like to underline that people involved in serious crimes are much more likely to have the means to circumvent technical and organisational security measures than normal citizens and businesses or even most small criminals.

The Directive does not provide for strong security measures with sufficient precision.

This brings me to the issue of outsourcing: The Data Retention Directive could have limited outsourcing as a security measure. However, it does not impose any specific requirements with regard to the storage of retained data. These are subject to the general rules of Directive 95/46/EC:

- ◊ Under that directive outsourcing is allowed, but should take place under stringent requirements, ensuring that the outsourcing company can effectively remain responsible, also for respect of security.
- ◊ Storage in another MS would in principle be possible, since under EU law there is a free flow of data.
- ◊ Storage in a third country would in principle also be possible, subject of course to the specific rules on Trans Border Data Flows.

Mr. President, Members of the Court,

I come to a conclusion.

The EDPS does not exclude that a well-defined obligation to retain telecommunications data may be justified under strict conditions, in

compliance with the requirements flowing from both Article 7 and Article 8 of the Charter.

Directive 2006/24/EC does not comply with these requirements. We mentioned that the directive requires the retention of data of ALL EU citizens whereas its effectiveness is not fully demonstrated, it makes detailed profiling possible, and there are no specified security requirements.

It is not sufficient for the EU legislator to adopt an instrument that allows for wide limitations on the exercise of fundamental rights and freedoms, without respecting the essence of those rights, and then basically assume that the 28 national legislators will repair this flaw.

This is a task of the EU legislator itself. It is not sufficient that a number of Member States ensure fundamental rights protection under their national laws.

I thank you for your attention.

Hielke HIJMANS,

agent of the European Data Protection Supervisor