SPEECH/10/723

Cecilia Malmström

Member of the European Commission responsible for Home Affairs

Taking on the Data Retention Directive

European Commission conference in Brussels

Brussels, 3 December 2010

Ladies and Gentlemen,

I am very happy to be here with you today, to say a few words on where the EU stands on data retention now and where we may be heading in the coming years.

Let me start by saying that it is encouraging to see so many participants from the law enforcement community, data protection authorities, the telecommunications industry, civil society as well as former colleagues from the European Parliament.

Your presence today confirms that data retention - the mandatory storage of telecommunications traffic and location data for law enforcement purposes - touches upon important, but also sensitive issues.

You represent a wide range of views on data retention. They differ on some points, but I hope it is fair to say that they all reflect the same basic concern: to ensure that people in the EU both feel and are in fact secure. Secure from crime and terrorism. Secure, at the same time, from excessive state intrusion into the private life of citizens. In other words, we probably all agree the EU must deliver security, but do so in a way that is proportionate to the risks at stake.

At the outset, let me make one thing clear – I am a Liberal politician and therefore cautious of any State collection of personal data. Data retention does raise issues of privacy, I am keenly aware of that.

But we have to recognise that data retention is here to stay, and for good reasons. Access to telecommunications data are, at least in some cases, the only way of detecting and prosecuting serious crime. And in some cases it can be vital to exclude individuals from crime scenes and clearing them of suspicion. We do need data retention as an instrument to maintain security in our Member States.

And EU rules on data retention are valuable in other ways. Harmonised provisions on issues such as purpose limitation, retention periods, and procedures for access to retained data help ensure that data is protected and privacy concerns addressed in all Member States.

Moreover, telecommunications providers would not be able to compete on an equal footing in the internal market without harmonised rules. The data retention directive was introduced partly for this reason. The need for a level playing field has not gone away!

Still, we must ask ourselves: what form should data retention take? How do we ensure that it does not go beyond what is necessary? How do we ensure that abuses of retained data are avoided?

Before moving on to those questions, let me share with you some preliminary results of the Commission's evaluation of the Directive. I see four important points.

First, on the usefulness of data retention for law enforcement, the information that the Commission initially received from Member States shows that national authorities very often request access to retained telecommunications data. 2008-2009 figures from 20 Member States show an average of 148 thousand requests per year in each Member State. 90 percent of those data were less than six months old when the authorities asked to see them. This gives an indication that the retention of data – even for a limited period of time – is useful for fighting crime: if the data were not helpful, law enforcement authorities would presumably not spend human and financial resources on requesting them in those numbers.

But to assess the necessity of data retention, I wanted more evidence from Member States. The Commission therefore asked for evidence on how widely retained data is actually used to prosecute serious crime, to protect victims and – let us not forget – also to clear innocent persons of suspicion. The information we received needs more analysis, but it does show that many criminal investigations would not have been successful, had it not been for data retention. One Member State informed us that its law enforcement agencies use retained data in more than 86% of cases resulting in criminal prosecutions. Several Member States pointed to the difficulty of dealing with cybercrime, an ever increasing threat to security, without data retention.

Secondly, we have looked at how Member States have implemented the Directive. Twenty Member States have implemented it by now. Several others are expected to do so soon. Although far from perfect, this situation is encouraging. The Directive is part of EU law and must – despite what some may regard as imperfections – be implemented by all Member States. If necessary, the Commission will take action before the European Court of Justice to ensure that happens.

That said, the Directive has not been implemented in exactly the same manner in those twenty Member States. Differences exist on several important points: how long data is retained, the purposes for which data can be accessed, the procedures which govern access to the data, what telecommunication operators are required to retain data, whether and how much those providers are compensated for the cost of data retention etc.

To give you just a few examples: while eleven Member States require data to be retained for one year, six Member States retain it for just six months, others again have a retention period of 2 years. In some Member States only police authorities can access retained data, in others customs and border guards may do so as well. Many Member States, but not all, require the involvement of a judge before access is granted.

Those differences in how the Directive has been implemented are due, more than anything else, to the fact that the provisions in the Directive are formulated in an open-ended, not to say imprecise, way. This raises the question whether the provisions should be made more precise, to ensure that we strike the right balance between law enforcement needs and privacy concerns in all Member States.

Thirdly, we have looked at the cost of data retention for economic operators. Of course security comes at a price, telecommunication providers have had to bear considerable costs. But I do not believe that the health of our telecom sector has been affected by the Directive to any significant degree. Operators in different Member States may have felt the impact of the Directive differently because of differences in how it was implemented. Again, this begs the question whether we need clearer rules, including on State compensation for the cost of data retention.

Finally, we have examined the impact of data retention on fundamental rights. Data retention raises sensitive issues about privacy and the protection of personal data. Those issues must be taken very seriously. Fortunately, the evaluation process has not revealed any concrete cases of law enforcement abusing their powers to access retained data and violate the right to privacy. But the retention of data is, in itself, a source of concern to citizens due to the risk of retained data being abused. The question is, what rules and legal guarantees do we need to limit the risk of abuses?

To sum up, the evidence the Commission has collected so far suggests that the data retention Directive has made a substantial contribution to security in the EU, and provided a more level playing field for telecom operators. The costs for operators have not been unacceptably high. Valid concerns over the impact of data retention on privacy remain, although there is no evidence that it has led to serious abuse in any concrete cases.

Ladies and Gentlemen - where does that leave us, what are the future perspectives?

As I said already, I am convinced that data retention is here to stay. But most, perhaps all, of us would agree that the data retention Directive leaves room for improvement!

Building on the evaluation report, which I expect to be published early next year, I therefore intend to prepare a proposal to amend the Directive. That proposal should cover all relevant issues. To name just a few:

We must reflect again on the purpose of data retention, including the types of crime that the Directive covers;

We may need to agree on more harmonised, and possibly shorter, retention periods;

We should consider defining who may access the data and according to what procedures. Should there be a central contact point in each Member State? Should judicial authorisation be compulsory? What about cases of urgent need for access?

We need to agree on whether operators should be compensated by the State for the costs incurred. I would favour a close look at possible ways of compensating them;

We need to ask what types of data to retain. I would be sceptical of enlarging the scope of the Directive, as suggested by for example the European Parliament in a written declaration to include forms of communication or types of data not already covered by the Directive. But we need an honest discussion about this.

And we need to address the argument that data retention should be replaced by a system of data freeze, or data preservation. I am not convinced that this would be an effective alternative. Data freeze will never bring back deleted data. Only data retention ensures that data which may one day be decisive – to prosecute or to clear a criminal – are available. I am afraid there are no easy choices or shortcuts here.

Let me conclude: today's conference marks the end of the Commission's evaluation process and the beginning of a new process leading, I hope, to a much improved EU data retention directive.

A directive which draws on a full and open public debate, which limits the purpose and scope of data retention to what is necessary, which contains all the necessary safeguards to protect against abuses, and which lays down clear rules for all Member States.

I will need your help - your technical expertise and your views - in the coming months to reach that objective. I look forward to working with you all!

Thank you very much!