

Brussels, 5 September 2003

**MEETING OF PARLIAMENT'S LIBE COMMITTEE,
9 SEPTEMBER 2003**

Speaking note for MR BOLKESTEIN on U.S./EU talks on PNR

Honourable Members of the European Parliament,
Ladies and Gentlemen,

1. PRELIMINARY REMARKS

I have come to you today to assess where we stand on transfers of Passenger Name Record data to the U.S., to consider what our options for action are and, together with you, to **devise solutions**. It is clear that the present situation – which is at best legally fragile – cannot be allowed to continue. The Commission is fully aware of this.

It is equally true – and I am confident that you, who have been following this matter very closely since February, will share my analysis – that there are no easy or "perfect" solutions.

Let me say straight away that the COM needs no reminding that it is the guardian of the Treaty; nor that

fundamental rights, our highest good, are at stake here.

But let's face it: we are confronted with competing, even to some extent irreconcilable concerns, all of which are legitimate in themselves. To quote an American author, H. L. Mencken: "*For every complex problem there is an answer that is clear, simple, and wrong.*"

The U.S. requirements raise a number of policy issues:

- Fight against terrorism;
- Right to privacy and fundamental civil liberties;
- Ability of our airlines to compete;
- EU/U.S. relationship in general and, last but not least;

The security and convenience of legitimate air travellers, including actual or potential European air transport and border security concerns

None of these angles **alone** – indeed **no** one-sided approach – would lead us to the optimum solution. In particular, what is urgently needed in my view is a

coherent EU policy on the use of PNR data for transportation and border security purposes. But I will come back to this when addressing the options for actions.

What has caused the problem is a conflict of laws, but not just that. There is no avoiding the fact that the U.S. has a **different approach** when it comes to the security of their homeland.

However, we must not exaggerate these differences. We are all solidly behind the U.S. in the need to combat terrorism. And we should not forget that the U.S. is not alone in thinking that the use of airlines Passenger Name Records is necessary for security purposes: Canada and Australia have already made similar requests, and others are expected to follow. **We must be realistic.** Security concerns do exist and they are not by any means an exclusively American obsession. Some Member States also use or are considering using Passenger Name Record data for border or aviation security purposes.

We are faced here with a truly international problem. As the COM has said from the start, we believe that

the best solution would be a multilateral one, and we are preparing to launch an initiative in the International Civil Aviation Organisation designed to bring this about.

2. COMMISSION'S ASSESSMENT OF THE STATE-OF-PLAY (EU-U.S. TALKS)

So let me turn to the COM's assessment of the **results of our talks** with the U.S.

It must be said that some real improvements in the way the U.S. process PNR data have been made – but unfortunately not to the point where the Commission can regard the requirements of “adequate protection” to have been met.

The main **improvements** (and I refer here to the U.S. "undertakings" of 22 May) are:

- That there be no electronic access to the PNR data held by the U.S. Customs and Transportation Security Administration by other agencies, and that onward sharing only be on a case by case basis;

- A considerable shortening of the periods during which data will be retained (from 50 to 6-7 years);
- And the appointment of a Chief Privacy Officer in the Department of Homeland Security who must report annually to Congress.

So there has been an effort to address our concerns.

Since May however, progress on the remaining issues has been rather disappointing. Of the long list of concerns expressed by our Data Protection Commissioners in June, **only one** has been resolved since then – albeit an important one: **as confirmed in Secretary Ridge's letter to me of 7 August**, the U.S. has agreed to filter and delete all data that Article 8 of the Directive defines as **sensitive**. For the rest, they have not been prepared to move much beyond their “undertakings” paper of 22 May.

Four shortcomings remain in particular:

- 1) Purpose limitation:** the U.S. do **not** want to limit their use of PNR to the fight against terrorism, but **want to cover** "other serious criminal offences"

and have not so far been prepared to narrow this further;

- 2) **Scope of data required:** the U.S. requires 39 different PNR elements, which it is hard to regard as proportionate to the purpose;
- 3) The still very long **data storage periods** (6-7 years); and
- 4) The insufficient legal bindingness of U.S. undertakings – hence our insistence, if rights are not actionable before U.S. courts, on independent extra-judicial redress mechanisms.

For all the reasons evoked, under present circumstances and based on U.S. undertakings obtained so far, the COM is **not in the position to make an 'adequacy finding'** regarding the level of protection provided by the American authorities.

The Directive of course gives the COM some latitude in the assessment of adequacy. However, based on *current* U.S. undertakings, an adequacy finding would

be vulnerable to legal challenge. This would get us nowhere in our search for greater legal certainty.

3. OPTIONS FOR ACTION

This brings me to the third and last part of my remarks: what are our options for action. It is clear, as I already said at the beginning, that the present situation cannot be allowed to continue.

I basically see only **three** possible courses of action:

- 1) The first possibility is to go on seeking improvements from the U.S. with the aim of reaching the point where we could make an adequacy finding. Obviously we should **persevere** with our efforts **and in this regard, I welcome the constructive tone of Secretary Ridge's letter. I hope to discuss the matter with Mr Ridge's deputy, Mr Asa Hutchinson, when he is in Brussels on 22 September.** But we cannot let this process go on indefinitely. We should set ourselves and the Americans a **clear deadline.**

2) The second kind of action of action open to us is to **enforce the law**. In present circumstances, this would **ideally mean stopping the data transfers**. As far as the Data Protection Directive is concerned, this is a job for the Member States and their data protection authorities. The COM's immediate role is to ensure that the *Member States* respect the Directive, not that the airlines do.

There is a second legal instrument that is relevant here: the Computerised Reservation Systems Regulation. If the data protection provision of this Regulation – namely Article 6 – is being breached, it is for the COM to take the necessary enforcement action. **At present, the Commission does not have clear-cut evidence of a breach, but is writing to the CRSs to obtain more information and to remind them of their obligations.**

Enforcement action is superficially attractive, but it is not clear that its consequences would be

those we sought. If the airlines complied and stopped giving access to their data, the first consequence would be so-called "secondary inspections" of arriving passengers in the U.S., with long waits and much inconvenience for travellers. Beyond that, we might see our airlines being fined or even having their landing rights withdrawn. Airlines might well therefore not comply, and it is not clear that the Member States would all take the same view in that case. Some would press on with enforcement actions against the airlines. Others, it is clear, would not. Most are rightly looking for a solution **at EU level**. This would surely be preferable. This would at least avoid selective pressure being applied on individual Member States.

3) This brings to me to the third and last option for action: namely to **negotiate a bilateral agreement** with the U.S. Such a bilateral agreement could be used to bridge the gap between the two legal systems, while ensuring the highest achievable level of data protection

for EU citizens. This would allow narrowly targeted derogations to be made from the Data Protection Directive, if necessary, while respecting of course the limits set by the European Human Rights Convention.

However, the Commission would be prepared to go down this path **only with the clear support of the Parliament and Council.** In addition, a number of conditions would need to be met:

- 1) First, a switch from "pull" to "push" as regards the method of transfer. Indeed, I think this is essential in *whatever* scenario we find ourselves;
- 2) Second, data protection arrangements in the U.S. that come closer to adequacy than they do currently; and
- 3) Third, a procedure on the EU side that would involve the European Parliament's assent, as required by Article 300, paragraph 3 of the Treaty.

Mr Chairman, Honourable Members, that is what I wanted to say. I now very much want to hear from you on what **you** consider the best way forward. I have promised to report back to the COM before the end of this month based on my discussions here and with Member States.