Statewatch Briefing

Public Hearing hosted by MEP Jan Philipp Albrecht
Speakers
Protection of Personal Data in Transatlantic Security Cooperation SWIFT, PNR & Co - which way forward?
8 April 2010

Speakers

• Peter Hustinx, European Data Protection Supervisor
• Edward Hasbrouck, PNR researcher at The Identity Project, San Francisco
• Paul de Hert, director of the Research Group on Fundamental Rights and Constitutionalism (FRC), Vrije Universiteit Brussel
• Patrick Breyer, legal coordinator, Working Group on Data Retention, Germany
• Despina Vassiliadou, EU Commission, DG Justice, Freedom and Security

Introduction

The LIBE Committee announced during its last meeting its intention to postpone the vote on the EU-USA PNR agreement, calling the Commission to put forward a more comprehensive measure defining common data protection terms.

The European Commission is therefore going to put forward a more coherent "package" which will include:

a) a Communication listing general standards that should apply to any PNR agreement (regulate external aspects)
b) a PNR directive which will be a "Lisbonisation" of the current agreement and
c) a recommendation for a negotiating mandate with the USA, CANADA and Australia on PNR.

There are several loopholes that have been identified by experts, academics as well as Members of the Parliament which refer to other on-going negotiations as well, namely the so-called SWIFT Agreement and the Framework Agreement on data protection and data sharing.

Different understanding of privacy and data protection

Privacy and data protection are two different albeit interlinked principles and this distinction needs to be applied in the internal and external dimension of EU.

The right to privacy is not absolute, in fact most of the emphasis is on the condition under which restriction could be imposed. The right to data protection always applies when personal data are processed. The European Court of Human Rights has emphasised that in applying data protection principles that Article 8 of the European Convention on Human Rights must also be respected.

This link becomes increasingly important in relation with data sharing measures and even more when they entails international agreements with third countries, such as in the case of Passenger Name Record (PNR).

In the area of EU-US cooperation, for example, the different understanding of data protection and privacy further complicate the issue, since the U.S. approach to privacy protection relies on industry-specific legislation, regulation and self-regulation whereas the European Union relies on a comprehensive privacy legislation.

Negotiators need to bridge these two approaches ensuring general adequate principles, which can then be applied to all specific agreements.

However, the transfer of personal data is already taking place without the existence of such an overarching agreement via the agreement provisionally implemented on PNR.

This approach is highly objectionable. It is necessary to make sure that the broad agreement is compatible with the EU-US general agreement on data protection and not the other way around, as highlighted by the European Data Protection Supervisor. Otherwise the risk of inconsistency between the general principles and their application to specific agreements becomes more than likely.

This risk is already a reality with the PNR Agreement, which currently entails a series of measures at risk of violation of human rights as enshrined in the European legislation and case law:

Computerised Reservation Systems (CRS) as the "brokers" between the airlines the customers and the security authorities

As Mr Edward Hasbrouck explained, PNR data are entered by travel agencies, travel websites and tour operators in a third-party “Computerised Reservation System” (CSR.

The CSR then send the PNR data to the Department of Homeland Security (DHS) and since three out of four servers are based in the USA (including an office of the major EU sever), DHS and others in the USA can have access to EU data, even when they refer to intra-Europe flights.

The current PNR agreement covers transfers of PNR data from the EU to the DHS, it does not cover DHS relations with CSR. Hence, as Mr Hasbrouck correctly pointed out, standard airlines business completely by-pass EU-US PNR agreement.

As far as the CRS are concerned the legal situation in the EU has been recently updated (February 4th, 2009) by Regulation 80/2009 on a Code of Conduct for computerised reservation systems and repealing Regulation 2299/89:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:035:0047:0055:EN:PDF

Art. 11, to which recital 21 refers, states:

> “1. Personal data collected in the course of the activities of a CRS for the purpose of making reservations or issuing tickets for transport products shall only be processed in a way compatible with these purposes. With regard to the processing of such data, a system vendor shall be considered as a data controller in accordance with Article 2(d) of Directive 95/46/EC.

2. **Personal data shall only be processed in so far as processing is necessary for the performance of a contract to which the data subject** is party or in order to take steps at the request of the data subject prior to entering into a contract.

3. Where special categories of data referred to under Article 8 of Directive 95/46/EC are involved, such data shall only be processed where the data subject has given his or her explicit consent to the processing of those data on an informed basis.

4. **Information under the control of the system vendor concerning identifiable individual bookings shall be stored offline within seventy-two hours of the completion of the last element in the individual booking and destroyed within three years**. Access to such data shall be allowed only for billing-dispute reasons.

5. Marketing, booking and sales data made available by a system vendor shall include no identification, either directly or indirectly, of natural persons or, where applicable, of the organisations or companies on whose behalf they are acting.

6. **Upon request, a subscriber shall inform the consumer of the name and address of the system vendor, the purposes of the processing, the duration of the retention of personal data and the means available to the data subject of exercising his or her access rights**.

7. A data subject shall be entitled to have access free of charge to data relating to him or her regardless of whether the data are stored by the system vendor or by the subscriber.

8. The rights recognised in this Article are complementary to and shall exist in addition to the data subject rights laid down by Directive 95/46/EC, by the national provisions adopted pursuant thereto and by the provisions of international agreements to which the Community is party.

9. The provisions of this Regulation particularise and complement Directive 95/46/EC for the purposes mentioned in Article 1.Save as otherwise provided, the definitions in that Directive shall apply. Where the specific provisions with regard to the processing of personal data in the context of the activities of a CRS laid down in this Article do not apply, this Regulation shall be without prejudice to the provisions of that Directive, the national provisions adopted pursuant thereto and the provisions of international agreements to which the Community is party.

10. Where a system vendor operates databases in different capacities such as, as a CRS, or as a host for airlines, technical and organisational **measures shall be taken to prevent the circumvention of data protection rules through the interconnection between the databases**, and to ensure that personal data are only accessible for the specific purpose for which they were collected."

It is worth noting that according to Art. 14 of the Regulation the activity of the CRS on the EU territory falls under the European Commission oversight and the Commission has the appropriate powers of control and can accept appeals against any infringement of the code of conduct:

> "In order to carry out the duties assigned to it by this Regulation, the Commission may, by simple request or decision, require undertakings or associations of undertakings to provide all necessary information, including the provision of specific audits notably on issues covered by Articles 4, 7, 10 and 11."

But the extent to which this oversight power can actually be enforced is questionable. This is because the Directorate General (DG) of the European Commission in charge of the CRS is DG Transport (DG TRAN) whereas the DG responsible for PNR is Justice, Liberty and Security (DG JLS). Hence, if the two DG do not coordinate effectively, it is very difficult for the Commission to carry on the investigative tasks mentioned in Article 14 and ensure that no infringement of the code of conduct takes place.

The proportionality principle governing the processing of personal data

According to Directive 95/46, Member States must respect the following principles in the processing of personal data: the purpose limitation, the data quality and proportionality principle, and the transparency principle.

Hence, proportionality is also one the criteria that allows for limitation of privacy. In order to deliver proportionality in practice it is necessary to provide answers to the following questions:

- What does "narrowly tailored request" mean?
- What does "case by case request" means?
- Does case refer to a specific individual or more, or rather any data of all individual falling under a specific criteria?

The proportionality principle may only function against evidence. However, the evidence of the necessity of such measure has not been demonstrated yet. On the contrary, using the words of the Director General of DG JLS, Jonathan Faull, during the LIBE Committee on 24 March 2010, any evidence must remain secret as a matter of national security.

The balance between the limitation of privacy and data protection rights and the implementation of security measures can be reached only if such measures are assessed against the actual and not the perceived or presumed impact that they have on security. Otherwise, the very principle of proportionality fails and with it the respect of individuals' fundamental rights.

The purpose limitation and the question of re-use

The question of proportionality is directly linked to the purpose of data sharing. The recital of the 2004 Agreement states that its purpose is "to prevent and combat terrorism and transnational crime". Hence, it is necessary to guarantee that when

investigations demonstrate that someone is not a terrorist but has committed other unlawful acts, (such as overstay or copyrights infringement) the data collected will not be used to trigger another procedure.

However, as Dr Patrick Breyer pointed out, the High Level Contact Group (HLGC) report of May 2008 “does not provide for restrictive and specific purpose limitation in that sense and thus fails to satisfy human rights requirements to the disclosure of personal information to foreign agents and states”.

Exchange of data between private and public sectors

Furthermore, by allowing the exchange of data between the private and public sectors the risk of breaching the purpose limitation is a given and extra specific legitimacy - in addition to that already required - should be provided in order to guarantee the full respect of data protection and privacy.

Profiling

Currently, no common definition of profiling exists mainly because there are many profiling activities (In this regard, the Council of Europe is preparing a report which, according to Ms Vassiliadou, will provide the guiding principle for the Commission’s future work).

Data profiling consists in using key words to generate new data so as to progress in data analysis. Hence, by using normal data there is the risk of generating sensitive data.

This “practice” has become increasingly popular among private companies in order to create a more tailored service to their clients. However, if these profiles are used for law enforcement purposes by public authorities, the same individual may be against it.

That is why, according to Prof. Paul de Hert the principles of data minimisation and purpose limitations should be included when dealing with data protection and privacy legislation.

However, this might not be enough especially when faced with the risks represented by the automated machine data selection - the European Commission claimed there should always be a person to take the final decision rather then a machine and this should avoid that profiling will lead to a direct effect to a person, despite evidence to the contrary that “machines” will determine responses to perceived “threats” (see EU Future Group reports).

Purpose limitation and profiling are even more delicate aspects once analysed together with the right to redress foreseen in the PNR agreement as well as in the work of the HLCG.

Right to redress and effective remedy

Everyone whose right to data protection and privacy have been violated must have the right to an effective remedy before and independent tribunal as guaranteed in Article 13 ECHR and Art. 47 of the Charter of Fundamental Rights of the European Union.

However, the judicial system of the United States does not provide effective remedy and the Annex to the HLCG report of October 2009 only provides for administrative redress which cannot be defined an effective remedy.

Despite these unresolved issued, the Commission and the Council of the EU are determined to carry on negotiations concerning the SWIFT agreement as well as the PNR agreement.

Undisclosed sources referred that during the EU-US JHA meeting which took place at Ministerial level on 8-9 April 2010 in Madrid, the European Commission is looking for solutions on the aspects where divergences between the EU and the USA exist such as the bulk data transfer, redress principle, purpose limitation and push/pull techniques.

It is regrettable that despite all the aforementioned loopholes, to use an euphemism, the Commission did not supported the approach by which first a general framework agreement on data protection and data sharing with the USA should be concluded and only afterwards - if considered necessary on the basis of evidence- specific agreements such as PNR and SWIFT should be negotiated. Even though the current proposal for a general agreement falls way short of being acceptable.

The European Commission argued that it considers that the SWIFT agreement will be reinforced by the conclusion of the EU US data protection agreement.

During the meeting, the USA not only denied the existence of differences on the understanding of principles related to data protection and privacy on the basis of the OECD guidelines (which the EU thinks is not the right basis), but also considered that the issues raised by the European side in relation to the SWIFT agreement are based on pure misconceptions on how the system works.

by Leda Bargiotti