EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

Public Seminar

PNR/SWIFT/Safe Harbour: ARE TRANSATLANTIC DATA PROTECTED?

(Transatlantic relations and data protection)

Monday 26 March 2007

15:00 - 18:30

Brussels
Hemicycle

(Paul-Henri Spaak Building)

INTRODUCTION

On the 14th of February the European Parliament adopted with a large majority a resolution on SWIFT and PNR which states *"...it is necessary to define with the US a common and shared framework to safeguard the necessary guarantees that are needed in the special EU-US partnership in the fight against terrorism, which could also deal with all aspects concerning the free movement of persons between the EU and the US and considers that, in this perspective, contacts should be strengthened between Parliament and Congress".*

In order to strengthen the transatlantic dialogue a LIBE delegation will contact the responsible committees of Congress to evaluate possible improvements of the current context. The Seminar intends to take stock of the factual and legal situation which identifies the transfer of personnel data to the USA for security reasons, particularly in the framework of:
- data of airline passengers (PNR)
- data related to financial transfers (SWIFT)
- data exchanged between private parties (Safe Harbour).

The Seminar will open (I) with a general presentation of both, the constitutional and legal context of data processed in Europe[1], and in the USA, as well as the applicable principles on the international level for transfer of personal data (principles of the OECD of 1980).

Afterwards panels will (II and III) will examine the PNR case and the SWIFT and Safe Harbour case. The objective is to collect as many facts and data as possible from the participants, concerning:
- the information given to the users and on the applicable contractual rules
- the amount of data collected for security reasons by the US authorities
- the problems which have arisen following the collection of data, and issues linked to processing these data
- the use and the dissemination of personal data
- how does the joint EU and US review work (see the PNR Agreement)
- rules on the redress mechanism (compensation)
- whether these data are still necessary and proportionate for the purpose of fighting terrorism?

During the debate we will also examine improvements which could be made to the internal EU and US legislation, as well as to the current forms of transatlantic cooperation with the goal of
- providing European citizens in the USA with the same legal protection as enjoyed by American citizens (the same way US citizens enjoy the same right of EU citizens when in Europe)
- who strengthening the judicial and police cooperation by the US and the EU and its Member States

We would like to invite to this Seminar the representatives from: the Council, the Commission and the US administration; national and European data protection authorities meeting in the Directive 95/46, Art. 29 Working Party[2]; economic actors and representatives from European and civil society concerned with PNR, SWIFT and Safe Harbour.

The Seminar is also open to representatives from the European as well as National Parliaments and Ministries of the Member States, considering their essential role in this domain.

To provide structure to the discussions the participants are invited to take account of some relevant questions which were raised in the recent European Parliament Resolution[3].

PRESS CONFERENCE
(14h15-15h00)

Press Conference given by Mr. Jean-Marie CAVADA, Chairman of the Committee on Civil Liberties, Justice and Home Affairs and Mr. Peter SCHAAR, Chairman of Article 29 Data Protection Working Party

OPENING REMARKS
(15h00-15h05)

INTRODUCTION

Welcome by Mr. Jean-Marie CAVADA, Chairman of the Committee on Civil Liberties, Justice and Home Affairs (5 min.)

PANEL SESSION I
(15h05 - 16h10)

EU-US DATA PROTECTION LEGAL FRAMEWORK AND INTERNATIONAL PRINCIPLES ON EXCHANGING PERSONAL DATA

The legal context of data processed for security reasons in the USA and in Europe and the principles applied to the international transfer of data (OECD principles of 1980)
Prof. Stefano RODOTÀ[4] (5-7 min.)
Chairman of Art. 29 WP, Professor of Law, Professor of civil Law, University of Rome.
What are the possible limitations of the combined Member States' Constitutional prerogatives and EU level requirements, and what are the possible means of cooperation between legislative and judiciary authorities in the field of data protection?
Prof. Spiros SIMITIS[5] (5-7 min.)
Professor of Law, Johann Wolfgang Goethe Universität Frankfurt am Main
What are the limits set by the OECD Principles of 1980[6] and the Convention 108[7] of the Council of Europe, and by EC and EU law regarding transfer of personal data to third countries, particularly to the US?
Prof. Francesca BIGNAMI[8] (5-7 min.)
Professor of Law, DUKE University, Durham USA
An analysis of the 'Privacy Act[9] (actual state and possible evolution); role of the Privacy officers in Federal Departments and foreseen proposals to establish an independent authority to oversee its implementation.
Prof. Marc ROTENBERG[10] (5-7 min.)
Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC (teaches information privacy law).
The Privacy Act and the data protection granted to non US citizens.

Questions and answers

PANEL SESSION II
(16h10-17h20)

PASSENGER DATA (CURRENT AND FUTURE PNR AGREEMENTS)

Mr. Peter SCHAAR (5-7 min.)
Chairman of Article 29 Data Protection Working Party, Directorate-General Justice, Freedom and Security, Data Protection Unit
Presentation of the position of the Art. 29 Working Party, on PNR[11]
Mr. Arnaud CAMUS, AEA representative (5-7 min.)
Problems encountered by airlines in relation to processing the passenger data.

Mr. Ben SIMMONS, Amadeus (5-7 min.)
Problems encountered by Amadeus in relation to data transfers/data security.
Dr. Gus HOSEIN*[12]*, Senior Fellow, Privacy International (5-7 min.)
Are US Airlines/passengers treated differently to their European counterparts in relation to PNR?
Mr. Barry STEINHARDT*[13]*, Director, ACLU Technology and Liberty Project (5-7 min.)
Concerns related to PNR and ATS, see the open letter sent to the EU Institutions[14]

Questions and answers

PANEL SESSION III
(17h20 - 18h00)

SWIFT AND SAFE HARBOUR

Co-chairing Mrs. Pervenche BERÈS and Mr. Jean-Marie CAVADA

Prof. Yves POULLET*[15] *(5-7 min.)
Professor at the University of Namur and Liege, Dean of the Faculty of Law of Namur, Director of the CRID
The framework of the treatment of data by multinationals in the EU and US. Possible legal conflicts in the treatment of personal data.
Mr. Peter SCHAAR Chairman (of the Art. 29 WP) (5-7 min.)
Presentation of the position of Art. 29 Working Party, on SWIFT and on exchange of data in the international framework.
SWIFT: Ms. Blanche PETRE (5-7 min.)
Presentation of SWIFT's understanding of their obligations under EU and US law.
European Bank Federation: Mr. Thorsten HÖCHE and Mr. Sébastien De BROUWER (5- 7 min.)
Obligations and contracts between banks, customers and the impact on SWIFT services.

Questions and answers

CONCLUDING REMARKS BY:
(18h00 - 18h30)

EDPS: Peter HUSTINX
The position of EDPS on the transfer of personal data in the PNR, SWIFT and Safe Harbour context
the Council Presidency: Mr Wolfgang SCHÄUBLE *(to be confirmed)*
Presentation on the actual state of negotiations with US Administration.
the Commission: Mr Franco FRATTINI *(to be confirmed)*
Presentation on its position on the subject outlined above
Closing remarks of President Jean-Marie CAVADA

ANNEX

PRACTICAL GUIDELINES FOR THE DEBATE

Presentations will be limited to 5-10 minutes (see programme for details).
During the discussion, so as to make it possible for the highest possible number of parliamentarians to intervene, speaking time will be limited to 2 minutes per contribution or question.
The floor will be given to Members in the order in which requests are received.
Speakers wishing to supplement their speeches may do so in writing by submitting documents (preferably in English or French) in advance to the secretariat (email: ip-libe@europarl.europa.eu). These documents will be circulated during the meeting.

IMPORTANT NOTICE FOR THOSE WISHING TO ATTEND THE HEARING

This seminar is open to the public. However, for security reasons, participants who do not have a European Parliament access badge must obtain a pass in advance. Those wishing to obtain such a pass should contact the seminar secretariat (ip-libe@europarl.europa.eu) **before 21 March 2007**. It is essential to provide us with your **full name, address and date of birth.** Without this information, the Security Service will not provide entry passes.

Seminar Secretariat	**Telephone**
Emilio De Capitani *Head of Unit*	+32.2.284.35.08
Martina Sudova *Administrator*	+32.2.283.14.76
Anita Bultena *Administrator*	+32.2.284.25.32
Olivera Mandic *Assistant*	+32.2.283.24.65
Maria Lazarova *Secretary*	+32.2.283.23.89
Anne De Coninck *Secretary*	+32.2.284.21.79
ADDRESS: European Parliament Rue Wiertz 60 RMD 01J032 - B-1047 Brussels	**E-MAIL** **ip-libe@europarl.europa.eu**

PANEL SESSION I: EU-US LEGAL FRAMEWORK AND INTERNATIONAL STANDARDS IN EXCHANGING DATA

More than six years after the September 11th 2001 attacks, it is time to look at both sides of the Atlantic, in the following areas:

a) If the measures taken in urgency after the attacks have proved their worth and to what extent they should be modified and confirmed (see the case of the Patriot Act in the United States and similar measures taken in Europe). The US has already started this reflection, Europe has yet to do so.

b) If a proper legal framework of co-operation between the US and Europe should replace the current ambiguous and random relationship based on multiple and very different instruments (only two of which are international agreements in due form :the EU-US agreements on mutual legal assistance and extradition, recently subjected to examination and ratification by Congress).

c) **If after the conclusion of the "Open Skies" agreement would it be possible to strengthen at the same time the security and the rights and freedoms of individuals who travel on both sides of the Atlantic ?**
Would it be possible to build a 'Schengen-like' zone based on common binding principles (to be transposed in the internal EU and US legislations) and on measures strengthening the mutual confidence one of which could take the form of common systems of arbitration ?

Obviously , the answers to these questions require the support of the US Congress.

From the EP side in particular as regards data protection, the main aim is to ensure that European citizens when in the US are not discriminated against (as is the case for US citizens in Europe).
First steps in this direction could be:
- extending the protection of the Privacy Act to ([16]) European citizens in the same way that US citizens are protected in Europe by Directive 95/46; and
- extending the visa waiver to all citizens of the European Union, in the same way that US citizens do not need a visa to go to Europe.

Is such a prospect possible having regard to the existing constitutional framework and the current principles at international level?

Which legislative modifications would be required within the EU and the US?

If the objective of a 'Schengen-like' area is shared also by the US Congress why not overcome the actual situation where the same data could be accessed under very different legal conditions and why maintain "executive" agreements lacking transparency and parliamentary supervision?

Would a common EU-US initiative be a possible term of reference for a worldwide solution as regards data protection against abuses by the private sector or the authorities?

PANEL SESSION II : EU-US AGREEMENT ON PNR

In the aftermath of the terrorist attacks of September 11th 2001, the United States passed a series of laws to enhance domestic security against terrorist threats. In this framework, air carriers operating passenger flights to the United States must make Passenger Name Record (PNR) information available. Airlines face sanctions in the US for non-compliance.

An Agreement and an Adequacy Decision on PNR were signed in May 2004 between the Community and the US. They were, however, annulled by the European Court of Justice on 30th of May 2006 because of the legal basis (1st pillar). Following this ruling of the Court the EU should negotiate a new Agreement on a correct legal basis. There has been an Interim Agreement in place since October 2006 which expires by the end of July 2007. It should be replaced by a new long-term Agreement.

The European Parliament has expressed its views on the PNR on many occasions.[1] The PNR Agreement has led to a situation of uncertainty with regard to the necessary data protection guarantees for data sharing and data transfer between the EU and the US for ensuring public security, and in particular preventing and fighting terrorism. Also the Interim PNR Agreement does not adequately respect the personal data of EU citizens. What can be expected from the future long term PNR Agreement for which the mandate has just been given (on 22 February 2007)?
Even though it has been in place for some years, this agreement still raises some fundamental questions, such as the following.

1. Why, three years on from the launch of the PNR agreement, has there not been an information campaign by airlines and US / EU authorities at European and national level to inform the travelling public of their rights and the manner in which passenger data are processed by US authorities ?

2. Why has there been only one (limited) joint EU/US review in four year? Given that the current Interim Agreement foresees a joint review, what are the contracting parties doing to realise this joint review prior to the conclusion of a new long-term agreement?

3. What has been the real economic organisational impact of the PNR agreement for the airlines and for the CRS located in Europe (AMADEUS)?

4. The US imposes on the airlines so-called watch lists ("no-fly list and selectee list)" against which they check for the presence of dangerous passengers. Why are these lists not sent to the European Border authorities? Has the EU checked on which legal basis the airlines process data on the watch lists?

5. In case of denial of boarding on European soil, how and to whom can a European citizen prove they are not the person on the "no-fly" list?

6. Which of the 34 data items have been the most frequently accessed and what problems have

[1] i.e. EP resolution on Swift, PNR and transatlantic issues, P6_TA- PROV(2007) 0039 and recommendation P6_TA-PROV(2006) 0354 of 7 September 2006.

been detected? Is there an evaluation planned to verify the need for so many data elements?

7. Apart from the data linked to the identification of the passenger, which PNR data are the most frequently accessed and which are very rarely accessed? How can a reduction of the data elements be achieved in view of the Canadian PNR Agreement which uses only 25 data elements, and functions well?

8. Even if there is no formal link between PNR and ATS or US Visit, it might be feared that the electronic retention period of personal data will be extended from 3 and half years to many decades. How can data subjects avoid abuses and consequences for them? Has the impact the proposed ATS might have on a future PNR Agreement been assessed?

9. The Congress has formally forbidden profiling and data mining techniques for US Citizens; are these techniques applied to Europeans and, if so, what is the impact? What assurances have been given by the US that the future ATS will not be used for profiling purposes?

10. The DHS Traveller Redress Inquiry Program (DHS TRIP) has recently been launched but without referring to the rights and redress mechanism foreseen in the Privacy Act. How does this protection work, and to whom does it apply? Which data protection norms apply?

11. Why has the PUSH system been postponed? What are the contracting parties doing to come now to a push solution as there are no technical obstacles for such a switch from pull to push?

12. Does the USA transfer PNR data to third countries (such as Russia, Pakistan, China...)?This is particularly important in light of the side letter which seems to derogate from the Undertakings given by the US and is in favour of a facilitated onward transfer of passenger data.

13. How has the PNR agreement been transposed so far in the EU countries?

AS FAR AS A FUTURE PNR AGREEMENT IS CONCERNED

1. The EU has recently adopted internal legislation on "APIS" data which are apparently more useful for identification purposes; would it not be enough to limit the future agreement to these data?

2. Other countries like Canada and Australia use some PNR data; would it not be better to refer to these models and have less invasive kinds of agreements?

3. The previous "adequacy finding" was annulled by the ECJ (in cases C-317/04 and 318/04 of 30 May 2006). How will the EU check if the data protection is adequate according to the Council of Europe Protocol 181([17]) and/or to the general principle on legal certainty?

4. The actual statute of the US "Undertakings" is less than compliant as far as the principle of legal certainty is concerned; how can the EU ensure that the future agreement will make them binding from an international perspective? And that a regular comprehensive supervision of

the implementation of the Undertakings is carried out?

5. Which conditions should be respected in authorising access by public authorities (other than the Border) to passengers' personal data?

PANEL SESSION III: SAFE HARBOUR AND SWIFT

CONTEXT: The Patriot Act gives the right to the US authorities to access certain data, held by the private sector, for the purpose of combating terrorism.
This exception being more and more frequent and widely used changes the situation which existed when the Commission adopted the "adequacy finding decision" on the Safe Harbour situation notably for:(a) the private multinational companies who process personal data of EU citizens on US soil; and (b) the European companies like Swift who for different reasons transfer or mirror their data in US territory.

After the September 11th terrorist attacks, the United States Department of the Treasury ("US Treasury") developed the "Terrorist Finance Tracking Program" ("TFTP") to identify, track, and pursue suspected foreign terrorists and their financial supporters.

Following press reports in June 2006, it was publicly disclosed that the US Treasury acting within the TFTP Program has served subpoenas on the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") - a Belgium-based company that operates a worldwide messaging system used to transmit, inter alia, bank transaction information.

The EP has no assured measures to ascertain how and how many data are accessed and at what conditions. The subpoenas are issued for the alleged purpose to find information about any transactions which relate or may relate to terrorism.

As a Belgian based cooperative, SWIFT is subject to Belgian data protection law implementing the Data Protection Directive (Directive 95/46/EC). SWIFT stores all financial messages for a period of 124 days at two operation centres (one in Europe and one in the United States). For data security purposes and to limit the impact of one server crashing, the European and US servers *mirror* (provide an exact copy of) the data held by the other.

The EP has been recently informed ([18]). that SWIFT envisages to subscribe to the "Safe Harbour" framework arrangements agreed between the EU and the US covering the transfer of personal data for commercial purposes to the US. This move will not solve the problem of access by the US Treasury to the SWIFT data, and a US/EU formal agreement defining that *"...processing of Swift data is proportionate and is otherwise in lien with EU data protection principles"* will be in any case necessary .

A formal agreement on the SWIFT case holds advantages for both the EU and US.

The US would obtain legal certainty that it can continue to process some SWIFT data in a clear framework, without too much fear of legal challenge, and European citizens would gain the assurance their data are processed in compliance with data protection principles. Preliminary discussions to this end began between the European Commission and the US Treasury in January 2007.

1. Why is the collection of financial data not happening in the official international framework (FTAT), and how could the EU and US agree that the collection and processing of data linked to financial transfers are effectively made according to these principles agreed at international level, and align their internal legislation (Bank Secrecy Act from the US, Directive 95/46/EC)?

2. Given that SWIFT is an international cooperative network with strong management offering services to several thousands of financial institutions and makes decisions which go beyond the normal and legally defined "margin for manoeuvre" within which a normal processor can make decisions, can one regard SWIFT as a controller with regard to processing of data via the SWIFTN and FIN?

3. Following the opinion the EDPS released on 1 February calling on the ECB to ensure that European payment systems (SEPA system) comply with data protection law, have the Art. 29 WP been solicited by the ECB for further advice? Would prior evaluation by the EDPS and by Art. 29WP be needed in order to guarantee the principles of proportionality, legitimacy, full transparency of data processing, respect of data subject's rights, external and independent public supervision?

4. To the Association of banks:

a) What measures have financial institutions taken so far to ensure that their processing of personal data via SWIFT complies with Directive 95/46/EC?

b) Regarding the obligation to inform the Bank customers of consequences of the processing of their data via SWIFT, what would happen if customers oppose such processing via SWIFT because of the consequences in terms of transfer to the US? What are the alternatives for the customers?

c) When Banks negotiated usage of this service with SWIFT, have they inserted in the contractual conditions that these data are to be treated by SWIFT within the strict respect of the European data protection principles?

d) Do the Banks inform their customers/counterparties that their data are processed by SWIFT and are stored in a database mirrored outside the EU, in a country where data are often accessed for security reasons by a third party under conditions very different from the ones used in Europe ?

e) Taking into account a possible conflict of law, as far as data protection is concerned, is it not preferable for SWIFT to have its second mirroring site in a country having the same level of data protection of the main one?

f) Swift is managing mainly financial transactions of international nature; therefore with the introduction of the Single European Payments Area (SEPA) and its implementation by SWIFT also the domestic financial transactions of any nature will be covered and possibly accessible by the US authorities. Against this background, have the European banks evaluated the potential data protection risks of this new situation of allowing a third country security service to have uncontrolled access potentially to every financial transfers (including those

linked to the activity of public authorities in the EU and its MS) ?

5. Question directed to SWIFT:

a) What is the basis of your services provided to banks: a generic commercial contract, a tailor made contract? Does such a contract refer to Directive 95/46/EC regarding protection of data? How far in the details?

b) The Council Presidency and the Commission have informed the EP of the possible use of the "Safe Harbour" agreement by SWIFT as a possible way to legalise their data mirroring in the US. Therefore the "Safe Harbour" agreement covering relations between two different subjects, one of them being on US territory, but SWIFT branch in the US having no legal personality, using the "Safe Harbour" does not appear to have any meaning.
Moreover the "Safe Harbour" does not cover the use of data for security purposes. As a result, the problems linked with the uncontrolled (at least from a European point of view) access by the US authorities remain unresolved. What would then be the benefit of such a step?

c) How many financial transactions are communicated to the UST?

d) What is the number of data related to transactions involving only EU counterparts transferred to the US mirror?

e) What is the percentage of data involving at least one of the US counterparts out of the total of data transferred to the US mirror?

f) Have you been threatened by possible sanctions by the US authorities in a case of non compliance to their requests?

g) Referring to the recent news of SWIFT opening its office in Brazil – and plans to open new branches/subsidiaries and informatics infrastructures in other countries/continents (like Japan, Russia, Asia), what will be the impact as far as data protection is concerned? Is the mirroring of data going to be put in place there too?

h) What about alternatives like:

- *coming back to the original functioning of SWIFT, where it did not dispose of the key to the messages. This would move the responsibility of communication of data to third parties to banks (and this should occur in compliance with the international agreements – Egmont network). This seems to be the most accessible and practicable solution for SWIFT, in terms of responsibilities and compliance with European law – by doing this, they might nevertheless have to provide for some added value services – could SWIFT confirm / develop on this? ;*
- *re-thinking the network: instead of a centralised network with two mirrors, opt for a decentralised network, where there would be no global copy of the whole database in one single place. What about the technical feasibility? The deadlines? We heard SWIFT is rethinking its technical infrastructure every five years. When is the next review?*

Transatlantic Data Protection : common principles but divergent practices

In democratic societies data protection ([19]) is a fundamental right of a crucial importance for individual who want to travel, to inform and express themselves, to associate and take part in the political life of a country without being subject to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". According to Art. 17 of the International Covenant on Civil and Political Rights "Everyone has the right to the protection of the law against such interference or attacks."

In Europe this fundamental right is expressly invoked

- at national level by several Constitutions ([20]) or by the jurisprudence of the Supreme Courts (as it is the case for Germany and France)
- at continental level by the Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, (ECHR) and by the Convention for the protection of individuals with regard to automatic processing of personal data
- at the European Community level by the Directive 95/46 **which, however, does not cover the judicial and police cooperation.** In the absence of self-determined standards the European Union and its MS have to follow according to art. 6 of the TEU the art. 8 of the ECHR and the constitutional principles.

The USA has no comprehensive data protection system on the contrary([21]), there is at federal and national level, a sectoral approach with a mix of legislation, regulation and self-regulation.
But even if, as far as data protection is concerned, the US and Europe are following different models, since the nineties they have had to co-operate in order to meet the threefold challenge of :

- the technological evolution linked to the internet which allows data to be everywhere
- the growing phenomenon of the multinationals which are able for functional reasons to process in a country the data linked to other countries
- the fight against international crime and terrorism.

The joint pressure of these three phenomena make it practically impossible to protect the data on the basis of a sole territorial and national approach.

Faced with this triple challenge, to avoid data protection being meaningless and to allow data to move freely, at least between countries with comparable protection, at the beginning of the 1980s, states defined principles to respect data transfers by means of:

- Convention 108 of 1981 of the Council of Europe, which developed the provisions of 'art. 8 of the European Convention of Human Rights; and
- the 'OECD [22] guidelines which the US also adhered to.

These principles concern primarily **the quality of data, the specification of purposes, limitations of use, guarantees of security, transparency, rights of the individual**, and the fact that the states had to adapt their national legislation.

However, the Member States of the EU and the US applied these principles in different ways. Moreover, the US did not give a specific right to the protection of data of non-US citizens (or those not legally resident in the territory of the US).

Under these conditions, the transfer of data could be considered possible especially within the framework of transfers within the private sector provided that they respected contractual clauses in line with the principles or voluntarily adhered to the "Safe Harbour" principles.

However, the problem of the adequacy of the US legislation remains as regards data protection when the data are collected for the purposes of combating terrorism and international crime.

In the aftermath of the September 11th 2001, the US decided to do the following.
a) - negotiate two international agreements with the EU as regards extradition ([23]) and mutual legal assistance ([24]) also covering equal conditions on data protection in the framework of judicial enquiries ([25]). These agreements also affect the rights of US citizens and were recently subjected for ratification by the US Congress.
In Europe these agreements were not subject to ratification by the EP but are in the course of ratification in several MS.

b) - within the framework of an international "light" agreement to obtain passenger data directly from the private sector (European airline companies) of individuals travelling to or through the US.

c) – to negotiate “executive” agreements:
- with Europol for the exchange of information and intelligence and to allow the exchange of personal data ([26]); and
- with Eurojust ([27]) which will foster the exchange of information between law enforcement communities in the US and the EU and will strengthen co-operative efforts to prevent and prosecute organised crime, human trafficking, cybercrime and terrorism.

d.) a great step forward would be the establishment of an independent data protection Commissioner in the US. The benefits of such a move are also repeatedly expressed by US companies and NGOs. It would facilitate the exchange of views with other parts of the world and secure an oversight of the processing of personal data regardless of the fact whether data are processed by commercial entities or by authorities. Such a step should be discussed with US Congress.

ENDNOTES

[1] The general Directive 95/46 on Data Protection is accessible at :
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
The specific Directive 2002/58 on Data Protection in the electronic communications
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
The EC Regulation 45/2001, applicable to the EC Institution is accessible at :
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:HTML

[2] The opinions of the WP 29 are available :
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

[3] The latest EP resolution on the PNR, Swift Case is at
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0039+0+DOC+XML+V0//EN&language=EN

[4] Profile at: http://www.mediamente.rai.it/mmold/english/bibliote/biografi/r/rodota.htm

[5] Profile of Professor Spiros Simitis:
Recent artcles: http://www.habeasdata.org/Interview-with-Spiros-Simitis

[6] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[7] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[8] See also http://www.law.duke.edu/fac/bignami/bibliography.html,
http://eprints.law.duke.edu/archive/00001603/

[9] The US Privacy Act of 74 is accessible at: http://www.usdoj.gov/oip/privstat.htm

[10] Marc Rotenberg Executive Director of the Electronic Privacy Information Center (EPIC)
http://www.epic.org/

[11] Presentation of the Position of the Article 29 Working Party from their internal working session (09h00-13h30, March 26, 2007)

[12] Gus Hosein Profile at : http://www.lse.ac.uk/people/i.r.hosein@lse.ac.uk/

[13] Prof Steinhardt profile at : http://www.aclu.org/about/staff/13282res20020211.html

[14] The open letter is accessible at http://www.privacyinternational.org/issues/policylaundering/ats/cavada.pdf

[15] Yves Poullet profile at :
http://www.e-administration.be/index.php?action=article&id_article=54007&id_rubrique=6709

[16] Another possible solution could be the creation of an indipendent Privacy Agency build on the the Privacy and Civil Liberties Oversight Board (whcih was created by the IntelligenceReform and Terrorism Prevention Act of 2004) as far as also EU citizens could refer to such a body.

[17] Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows)

[18] See The letter sent to President Cavada by the Council Presidency and by the Commission on the ongoing dialogue with the US counterpart on SWIFT

[19] For a general overview of Data protection see on the LIBE site the following page :
http://www.europarl.europa.eu/comparl/libe/elsj/charter/art08/default_en.htm

[20] Art. 10 de la Charte des droits et libertés fondamentaux de la République tchèque, / Art. 42 de la Constitution de la République d'Estonie, / art. 9a Constitution de la République hellénique, / Art.18 Constitution du Royaume d'Espagne, / Art. 22 Constitution de la République de Lituanie, / Art. 59 Constitution de la République de Hongrie, / art.10 Constitution du Royaume des Pays-Bas / Autriche - Lois constitutionnelles fédérales.Loi relative à la protection des données personnelles du 18 octobre 1978/ Art.51 Constitution de la République de Pologne./ Art.35 Constitution de la République portugaise / Art.38Constitution de la République de Slovénie/ Art.19Constitution de la République Slovaque/ Art.10Constitution de la Finlande / Art.3 Constitution du Royaume de Suède/ Art.13 et 15 Constitution Italienne...

[21] See for instance : http://datalib.library.ualberta.ca/publications/iq/iq22/iqvol223stratford.pdf

[22] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[23] The Extradition Agreement between US and EU is:
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf

[24] The Mutual Legal Assistance Agreement between US and EU is :
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00340042.pdf

[25] *DRAFT AGREEMENT ON MUTUAL LEGAL ASSISTANCE BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION. Art3 P. 1 lettre f) Subject to Article 9, paragraphs 4 and 5, Article 9 shall be applied in place of, or in the absence of bilateral treaty provisions governing limitations on use of information or evidence provided to the requesting State, and governing the conditioning or refusal of assistance on data protection grounds.*

Article 9: Limitations on use to protect personal and other data
1. The requesting State may use any evidence or information obtained from the requested State:
a) for the purpose of its criminal investigations and proceedings;
b) for preventing an immediate and serious threat to its public security;
c) in its non-criminal judicial or administrative proceedings directly related to investigations or proceedings:
i) set forth in subparagraph (a); or
ii) for which mutual legal assistance was rendered under Article 8;
d) for any other purpose, if the information or evidence has been made public within the framework of proceedings for which they were transmitted, or in any of the situations described in subparagraphs (a), (b) and (c); and
e) for any other purpose, only with the prior consent of the requested State.
2. a) This Article shall not prejudice the ability of the requested State to impose additional conditions in a particular case where the particular request for assistance could not be complied with in the absence of such conditions. Where additional conditions have been imposed in accordance with this paragraph, the requested State may require the requesting State to give information on the use made of the evidence or information.
b) Generic restrictions with respect to the legal standards of the requesting State for processing personal data may not be imposed by the requested State as a condition under subparagraph (a) to providing evidence or information.
3. Where, following disclosure to the requesting State, the requested State becomes aware of circumstances that may cause it to seek an additional condition in a particular case, the requested State may consult with the requesting State to determine the extent to which the evidence and information can be protected.
4. A requested State may apply the use limitation provision of the applicable bilateral mutual legal assistance treaty in lieu of the present article, where doing so will result in less restriction on the use of information and evidence than provided for in this article.
5. Where a bilateral mutual legal assistance treaty in force between the United States of America and a Member State on the date of signature of this Agreement, permits limitation of the obligation to provide assistance with respect to certain tax offences, the Member State concerned may indicate, in its exchange of written instruments with the United States described in Article 3, paragraph 2, that, with respect to such offences, it will continue to apply the use limitation provision of that treaty.1(1 This paragraph is intended to apply solely to Luxembourg.)
EXPLANATORY NOTE On Article 9. Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. A broad, categorical, or systematic application of data protection principles by the requested State to refuse co-operation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may as such not be imposed as additional conditions under Article 9(2a).

[26] US EUROPOL (not published on the EU, but published on the Europol Site)
http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf
http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf
on the Council Register
http://register.consilium.europa.eu/pdf/en/02/st15/15231en2.pdf
http://register.consilium.europa.eu/pdf/en/02/st14/14237-zzen2.pdf
http://register.consilium.europa.eu/pdf/en/02/st14/14237-r1en2.pdf

[27] US Eurojust (still not published on the EU OJ or Eurojust site : version accessible on the Council register)
http://register.consilium.europa.eu/pdf/en/06/st12/st12426.en06.pdf
http://register.consilium.europa.eu/pdf/en/06/st12/st12426-re01.en06.pdf