ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate-General for Internal Policies
Directorate C - Citizens' Rights and Constitutional Affairs
Policy Department C.: Citizens' Rights and Constitutional Affairs Unit

The European Parliament Civil Liberties, Justice and Home Affairs Committee (LIBE) Visit within the framework of the EU-US Transatlantic Legislators' Dialogue 15-18 April 2007

Background note and information sheets on:

1. Open issues in the EU-US Transatlantic Legislators' Dialogue as far as the freedom, security and justice policies are concerned
2. Transatlantic Data Protection: common principles but divergent practices
3. Specific issues :
- Visa Waiver Programme (VWP)
- Data Sharing / Data Mining
- Electronic Visa Application Form (EVAF)
- Privacy and Civil Liberties Oversight Board in the US

Joanna APAP
and
Emilio De Capitani

joanna.apap@europarl.europa.eu - www.europarl.europa.eu
B-1047 Brussels - Tel +32 2 28 32105 - Fax +32 2 28 32365
F-67070 Strasbourg - Tel +33 3 88 1 72662 - Fax +33 3 88 1 79804

Open issues in the EU-US Transatlantic Legislators' Dialogue as far as the freedom, security and justice policies are concerned

1. During this visit the Civil Liberties, Justice and Home Affairs Committee (LIBE) will meet different legislators from Congress to discuss certain cross-cutting issues which come within the legislative competence of mutual committees regarding Transatlantic Cooperation.
This dialogue will be extremely useful considering that Congress will shortly revise the principal issues of The Patriot Act. This is a legislative measure which has had a very significant impact on non-US citizens (or illegal American residents.)

2. It is worth mentioning that already in December 2001, two months after its adoption, the European Parliament ([1]) had raised profound reservations about the impact certain issues would have, such as the Patriot Act and the US President's executive order on military tribunals.
On this occasion the EP demanded notably :
"-not to limit in a disproportionate manner data protection standards (even if under a sunset clause) on electronic surveillance provisions,
- not to admit any discrimination between third-country and non-third country citizens that would be contrary to the ECHR,
- to guarantee the protection of fundamental rights as regards the monitoring of communications between a prisoner and an attorney,
- the procedural guarantees to a fair trial, as consolidated by the European Court of Human Rights;"

3. In the succeeding years, European Parliament's reservations proved to be well-justified as it appeared from the US Supreme Court Judgements as well as from the Congress legislation about the question of judicial security and the treatment of prisoners at Guantanamo.
Therefore, according to the European Parliament, the situation is still far from being what a partnership between the EU and the USA should be notably having regard to :
- the phenomenon of extraordinary renditions which could have taken place on European territory (cf. the temporary committee CIA's resolution)
- the possible violations of the principals of protection regarding personal details which have been repeatedly collected by the US administration (cf. the agreement on PNR and the US Treasury direct access to the worldwide SWIFT system for financial transfers).

---

[1] See EP Resolution **on EU judicial cooperation with the United States in combating terrorism accessible** http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2001-0701+0+DOC+XML+V0//EN&language=EN . According to this text the EP considered "*... that the US Patriot Act, which discriminates against non-US citizens, and President Bush's executive order on military tribunals are contrary to the principles established above;*
3. Considers that, such being the legal situation, legal problems could arise from the fact that the USA considers terrorists as war criminals, whereas this is not the case in the EU; considers that, therefore, no extradition could be allowed to the US from Member States for people who are to be tried before military tribunals;
4. Expresses concern at the fact that the President's executive order does not specify the limits on the court's jurisdiction, makes no provision for the presumption of innocence and the right to an impartial judge and, above all, allows sentences, including capital punishment, to be decided by a two-thirds majority;
5. Reiterates its request for a complete abolition of the death penalty in the USA and reminds Member States that they are bound not only on the basis of their individual ratification of Protocol 6 of the ECHR but also as members of the Union, in accordance with Article 6 of the Treaty; a general EU-USA agreement cannot therefore be reached; extradition cannot take place if the defendant could be sentenced to death;
6. Requests that expulsion or deportation proceedings should not be used as "disguised" extradition proceedings, and calls on the EU to guarantee European data protection standards that are proportionate, effective and of limited duration and to ensure that no mandatory retention of data be allowed, which would undermine rights and guarantees;

- and, last but not least, the current discriminatory attitude towards European citizens from the countries who do not enjoy the US visa waiver programme (even if for the time being the EU does not demand visas from US citizens visiting Europe.)

4. 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) Have the measures taken in urgency after the attacks proved their worth and to what extent should they be modified and confirmed?
The Patriot Act in the United States and similar measures aimed at enhancing security have been taken in Europe in the years. The US has already started this reflection; Europe has yet to do so.
b) Should a proper legal framework of co-operation between the US and Europe replace the current ambiguous and random relationship based on multiple and very different instruments?
There is an urgent need for such a Transatlantic legal framework, to be developed in a more systematic and transparent manner than the current "executive" agreements on the use of Passenger Name Records Data (PNR) or the practices introduced by the US Treasury to data processed by the SWIFT system without clear rules on access and treatment.

5. It has been recently proposed by the US administration to link the freedom of movement of individuals (visa waiver) with the need to strengthen the information sharing for security purposes. This move has already been developed in Europe in the framework of the Schengen cooperation which is build on mutual trust, non-discriminatory principles, solid data protection safeguards and a credible system of arbitration. If these conditions exist at the transatlantic level would the Congress accept to build a "Schengen like" area founded on the the EU/US agreements on extradition and mutual legal assistance and the Open Skies agreement ?

Would the Congress accept the principle that European citizens when in the US are not discriminated against, as it is the case for US citizens in Europe?

Would it be possible to extend the protection of the Privacy Act[2] to European citizens in the same way that US citizens are protected in Europe by Directive 95/46 and 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 ?

EDC

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

Transatlantic Data Protection: common principles but divergent practices

In democratic societies data protection[3] is a fundamental right of crucial importance for individuals 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".

However, differences between the EU and US with regard to the respective approach of protecting data privacy are more than theoretical.

In Europe this fundamental right is expressly invoked:

- at the national level by several Constitutions[4] or by the jurisprudence of the Supreme Courts (as it is the case for Germany and France);
- at the continental level by 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 Art. 8 of the Charter of Fundamental Rights of the European Union[5] and by the Directive 95/46 which, however, does not cover judicial and police cooperation.

In the absence of self-determined standards the European Union and its Member States have to follow and adhere to Art. 6 of the TEU, Art. 8 of the ECHR, and the constitutional principles.

The USA has no comprehensive data protection system on the contrary[6] there is at federal and national level, a sectoral approach with a mix of legislation, regulation and self regulation.

Moreover, Europeans reserve a deep distrust for corporations, while Americans are far more concerned about their government invading their privacy. As a result, U.S. federal agencies have been given little power to limit the potentially privacy-invading behaviours of private companies. The Federal Trade Commission, the agency charged with protecting U.S. citizens from such intrusions, rarely acts against U.S. firms. When it does, its remedies are generally limited to small fines and out-of-court settlements.

Each EU Member State, on the other hand, has a Data Protection Authority to monitor corporate behaviour. Consumers can appeal to the authority, which in some countries boasts far-ranging subpoena power. Fines for infringements are common.

---

[3] 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

[4] 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...

[5] Even if the Charter is not a legally binding text, one has to consider that it codifies the **common** constitutional values of **all** Member States.

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

In the EU, for example:

- Personal information cannot be collected without consumers' permission, and they have the right to review the data and correct inaccuracies.
- Companies that process data must register their activities with the government.
- Employers cannot read workers' private e-mails.
- Personal information cannot be shared by companies or across borders without express permission from the data subject.
- Checkout clerks cannot ask for shoppers' phone numbers.

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 one country the data linked to other countries;
- the fight against international crime and terrorism.

The joint pressure of these three phenomena makes 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[7] 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"[8].
Firms that pledge to follow these principles receive Safe Harbour from the application of the European Directive. The principles of the Agreement are binding on companies and businesses must choose whether they will be monitored and enforced by self-regulation or self-certification. Under self-regulation, the company agrees to comply with the principles and joins an independent dispute settlement body, which includes a range of private organizations. The Federal Trade Commission agrees to act as a regulatory backstop, monitoring firm compliance with their self-regulatory agreements. Because the Federal Trade Commission jurisdiction does not extend to financial services or telecommunications these sectors are excluded from the Agreement.

[7] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
[8] The Safe Harbour Principles are set in the Safe Harbor Agreement that was concluded in July 2000, and went into force in November 2000. A summary of the Safe Harbor Principles is available at: http://www.ita.doc.gov/td/ecom/shprin.html.

A 2004 review of the Agreement's implementation found that 75% of firms are self-certified, *de facto* placing themselves under the supervision of data privacy authorities in Europe. However, U.S. companies have expressed concern that the obligations of the agreement are not clear and that it creates a rather complicated framework to comply with European demands.

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[9] and mutual legal assistance[10] also covering equal conditions on data protection in the framework of judicial enquiries. 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[11]; and
   - with Eurojust[12] 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.

[9] The Extradition Agreement between US and EU is:
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf
[10] 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
[11] 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
[12] 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

Visa Waiver Programme (VWP)

The Visa Waiver Program (VWP) is a program of the United States of America which allows citizens of specific countries to travel to the US for tourism or business for up to 90 days without having to obtain a visa. All countries participating in program have a high Human Development Index HDI and most are regarded as developed countries.

Not all EU member states participate in the Visa Waiver Program.

Currently 12 EU Member States (Greece, Malta, Cyprus, Bulgaria, Romania, Slovakia, Czech Republic, Poland, Hungary, Latvia, Lithuania and Estonia) are not part of the Visa Waiver Programme and therefore their nationals are required to go through the relatively lengthier procedure of visa application to travel to the US even for a visit of less than 90 days.

By contrast, US citizens do not need a visa to enter any of the 27 EU Member States.
In their meeting with Secretary Chertoff on 5th April 2007, Vice President Frattini and Minister Schäuble have again stressed the importance of equal treatment by the US for all EU Member States and urged substantial progress regarding visa-free travel for all EU citizens.

- What agreement can therefore be envisaged between EU-US to eliminate the divide of the EU member States into two groups - those exempted of visas for travel under 90 days and those who are still subject to such visa requirements?

The key to a possible solution so far seems to be further data sharing (explained in the next section)

- Would further data sharing truly bring about more security or rather the possibility of higher risks of privacy intrusion for EU citizens?

- Would further one-way data sharing be an adequate solution to the lack of reciprocity from the US to the EU?

The revision of US legislation concerning conditions for participation in the visa waiver eventually for all 27 Member States falls fully within the framework of European Community competence.

Requirements for Visitors entering the US under the Visa Waiver Program

Despite the lack of requirement of a Visa to enter the US for less than 90 days, visitors entering the US under the VWP still need to meet certain requirements and are subject to a number of controls.

The October 2001 USA Patriot Act (public law 107-56) required visitors entering the United States under the VWP to possess machine-readable passports, which have one or two lines of letters, numbers, and hatch marks at the bottom of the photo page that can be read by optical scanners. Department of Homeland Security (DHS) regulations also established that each VWP applicant, including children, must present an individual machine-readable passport.

The new procedure ended the prior practice of allowing family members to apply for admission under one passport. (Machine-readable passports typically have space in the machine-readable zone for data on only one traveller.) The original deadline for implementing the new regulations was October 1, 2003, but technical problems led the administration to invoke a congressionally authorized waiver and extend the deadline for almost all VWP countries to October 26, 2004.

Under the Enhanced Border Security and Visa Entry Reform Act, Congress required all VWP participants to use biometric passports by October 26, 2004, as well. Passports containing biometric data (sometimes known as e-passports) have embedded electronic chips that contain a computerized record of observable biological features to identify the owner. These features can include fingerprints, iris or retina patterns, and as many as 1,800 facial characteristics.

Whereas machine-readable passports merely allow agents to verify a traveller's name, biometric data allow them to verify a person's identity. Using this information rather than name-based watch lists is thought to avoid the problems that arise when the name of an innocent person resembles that of someone on a watch list.

The United States and other countries adhere to the international technical standards for biometric data established by the International Civil Aviation Organization, a United Nations agency. These criteria include measures to promote the interoperability of contact-less chips and passport readers as well as to protect biometric data from unauthorized use. In May 2003, the International Civil Aviation Organization selected facial recognition as the required globally interoperable biometric.

The varying progress VWP countries have made in developing secure passports has required the United States to show flexibility in implementing the programme.

At present, VWP travellers who obtained machine-readable passports before October 26, 2005 are not required to have the digital photograph or contact-less chip. Foreign passports issued, renewed, or extended between October 26, 2005, and October 25, 2006, must be machine-readable and include a digital photograph printed on the data page. Passports issued, renewed, or extended on or after October 26, 2006, must be machine-readable and include the integrated chip.

VWP travellers are automatically enrolled in the DHS U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) programme. Under this programme, U.S. Border Patrol officers make inkless digital scans of two fingers and digital photographs of the face of each person applying for entry to the United States to ensure that the individual is the same person to whom the State Department issued a visa. The applicant's biometric and biographic data are also checked against the FBI criminal database and against terrorist watch lists, including the DHS automated biometric identification system, IDENT. The US-VISIT technology allows agents to scan travellers' information electronically from the visitor's travel documents (such as the I-94W), saving time and increasing accuracy. Except for diplomats, children under the age of 14, and passengers older than 79, all VWP travellers became subject to US-VISIT processing starting September 30, 2004.

Privacy Concerns

- What is the delimitation of access of data by competent authorities and other bodies in the US regarding data entered into the VWP?
- Which are the safeguards to protect the privacy of VWP applicants?

Data Sharing

Information Sharing Environment. The October 2001 USA Patriot Act (public law 107-56) foresees, and aims for, information sharing between law enforcement officials. In August 2004 an executive order - the Intelligence Reform and Terrorism Prevention Act - to strengthen the sharing of terrorism information was adopted.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 sets out the framework to establish the Information Sharing Environment in the US Federal Government "*in order to further strengthen the effective conduct of United States intelligence activities*".

The law grants the President authority to "*create an information sharing environment (such as passenger name records - PNR and Automated Targeting Systems - ATS) for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties*."[13]

Two techniques of data sharing systems are possible: - PULL and PUSH Systems

A pull system allows the requesting authority to directly access an external database to reach the data targeted. This gives less power to the party from whom data is requested to control what data is actually passed on to the requesting authority and therefore offers less guarantees for the protection of data. The current system envisaged for EU-US data sharing is a pull system and the US government seems to favour this method as it is less expensive, requires less technical infrastructure and more rapid access.

A push system offers a higher level of data protection and therefore may be preferable as the requested authority would have to send the selected data to the requesting authority. This is the system that is currently used for data sharing between EU and Canada (the EU-Canada agreement also collects significantly less fields of information). It is also efficient; the required technology to enable such a system already exists and it gives better control of data protection.

The White House has issued a Memorandum for the Heads of Executive Departments and Agencies setting out Guidelines and Requirements in Support of the Information Sharing Environment.[14] The Guidelines make clear that there is an obligation to "protect the information privacy rights and other legal rights of Americans."[15] However, the privacy rules that followed from the Guidelines were harshly criticized by privacy experts as undermining both statutory and Constitutional protections for privacy.[16] The Privacy Guidelines for the Information Sharing Environment do not provide legal protections for non-Americans.

Privacy Concerns

The Passenger Name Records (PNR)

In November 2001 the US Congress adopted the Transportation Security Act, as part of a package of measures to fight the terrorism, that ask to the air companies to provide the US Bureau of Customs

[13] Sect. 1016(b)(1). See generally, Office of the Director of National Intelligence, "Information Sharing Environment: Implementation Plan," (Nov. 2006), http://www.dni.gov/press_releases/ISE-impplan-200611.pdf

[14] Available at http://www.fas.org/sgp/news/2005/12/wh121605-memo.html.

[15] Sect. 2(e).

[16] "Civil Libertarians Protest Privacy Policy: New Guidelines Do Little to Protect Established Rights, White House Board Told," The Washington Post, Dec. 6, 2006, at A11, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/05/AR2006120501287.html

and Border Protection (CBP) an electronic access to their system of booking to the data of the passengers (the so-called Passenger Name records).

Given the sensitiveness of the issues at stake as well as the conflicts between the EU data protection provisions and the US requirements, the negotiations ended only in December 2003 and the first Agreement was signed in May 2004.

Under the U.S.-E.U. agreement, up to 34 types of information can be collected, including names, credit card data and flight itineraries. Sharing and use of the information is said to be restricted. The agreement is currently being renegotiated.

Concerns have been expressed in the European Parliament, in the context of the new agreement being renegotiated, regarding the breadth of the scope of information requested as well as the lack of clarity as to which agencies in the US will have access to such shared data.

Considering the Open skies agreement, the need for such privacy protection safeguards is urgent.

Automated Targeting System (ATS)
The Department of Homeland Security (DHS), Customs and Border Protection (CBP) have developed the Automated Targeting System (ATS). ATS is one of the most advanced targeting systems in the world. Using a common approach for data management, analysis, rules-based risk management, and user interfaces; ATS supports all CBP mission areas and the data and rules specific to those areas.

ATS is an Intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP. In this way, ATS allows CBP officers to focus their efforts on travellers and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveller, import, or export in context with previous behaviour of the parties involved. It is a system of profiling. Every traveller and all shipments are processed through ATS, and are subject to a real-time rule based evaluation.

In December 2006, it was reported that a system designed to assign risk ratings to cargo entering the United States was also being used to assign terrorist ratings to travellers. Such profiling of travellers would violate section 514 of the Department of Homeland Security Appropriations Act. According to one report, "The Homeland Security Department's newly revealed computerized risk assessments of international travellers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." [17] The U.S. Customs and Border Protection agency disputes this interpretation of the law.[18] The Department of Homeland Security has described the Automated Targeting System as "one of the most advanced targeting systems in the world."[19]

In an open letter to the chief privacy officials of 27 countries and to the LIBE Committee Chairman Mr Cavada, the American Civil Liberties Union and London-based Privacy International said the Automated Targeting System violated the October data-sharing accord, U.S. law and European data-protection laws.

[17] "Traveler Risk System May Violate Ban," Associated Press, Dec.7, 2006.
[18] "Facts Concerning the Automated Targeting System – CBP.gov," Dec. 8, 2006, http://www.cbp.gov/xp/cgov/newsroom/highlights/cbp_responds/facts_automated_targeting_sys.xml
[19] Dept. of Homeland Security, "Privacy Impact Assessment for the Automated Targeting System," (Nov. 22, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

The system's creation of terrorist risk assessments on all passengers, the storing of profiles for as long as 40 years, and the fact that passengers have no right to see, modify or correct the information violates the agreement, the groups said. "The ATS is a clear threat to privacy and human rights," Simon Davies, the director of Privacy International and Barry Steinhardt, the America Civil Liberties Union (ACLU)'s Technology and Liberty Project director, said in the letter.

According to a Department of Homeland Security spokesman, the programme did not violate the requirement that European passenger data be stored for 3 1/2 years at the most. He said the U.S.-E.U. agreement stipulates that some information may be kept for less than 40 years.

The air-passenger profiling programme has been operating for about 10 years, but its existence was not widely known until November 2006, when it was described in the Federal Register

Concerns also have been raised in Congress and by privacy advocates that information can be shared with a wide range of federal, state, and local government agencies for purposes other than border security and that the passenger assessments violated a congressional ban on developing such programmes.

Key questions which call for further discussion on data sharing are proper safeguards and proportionality.

Data Mining

Data mining (DM), also called Knowledge-Discovery in Databases (KDD) or Knowledge-Discovery and Data Mining, is the process of automatically searching large volumes of data for patterns using tools such as classification, association rule mining, clustering, etc. Data mining is a complex topic and has links with multiple core fields such as computer science and adds value to rich seminal computational techniques from statistics, information retrieval, machine learning and pattern recognition.

Data mining has been defined as "the nontrivial extraction of implicit, previously unknown, and potentially useful information from data" and "the science of extracting useful information from large data sets or databases". It involves sorting through large amounts of data and picking out relevant information.

Data mining identifies trends within data that go beyond simple analysis. Through the use of sophisticated algorithms, users have the ability to identify key attributes of business processes and target opportunities.

The term data mining is often used to apply to the two separate processes of knowledge discovery and prediction (including profiling). Knowledge discovery provides explicit information that has a readable form and can be understood by a user. Forecasting, or predictive modeling provides predictions of future events and may be transparent and readable in some approaches (e.g. rule based systems) and opaque in others such as neural networks.

Privacy concerns

There are privacy concerns associated with data mining - specifically regarding the source of the data analysed.

Essentially, data mining gives information that would not be available otherwise. It must be properly interpreted to be useful. When the data collected involves individual people, there are many questions concerning privacy, legality, and ethics.

A report from the Congressional Research Service in January 2007 raised new questions about the extent of data mining in the federal government.[20] Concern has also been raised about the ADVISE ("Analysis, Dissemination, Visualization, Insight and Semantic Enhancement") programme, which collects and analyze vast amounts of information on typical Americans.[21]

The Homeland Security Department began developing ADVISE in 2003, the same year that Congress cancelled funding for another extensive data mining programme Total Information Awareness over privacy concerns. Legislation was introduced in the Senate that would require annual public reports from "the head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining." The Federal Data Mining Reporting Act of 2007 was included in S 4, which passed the Senate on March 13, 2007.

[20] Congressional Research Service Report, "Data Mining and Homeland Security: An Overview" (Jan. 18, 2007), http://www.fas.org/sgp/crs/homesec/RL31798.pdf

[21] "New Profiling Program Raises Privacy Concerns," *The Washington Post,* Feb. 28, 2007, at D3, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/27/AR2007022701542.html

Electronic Visa Application Form (EVAF)

As of October 1, 2006, all applicants worldwide who wish to apply for tourist, student, or other non-immigrant visas to the United States must complete the visa application form on the internet using the Electronic Visa Application Form, or EVAF.

U.S. non-immigrant visas are required to submit an Electronic Visa Application Form, completed on-line at http://evisaforms.state.gov, in order to apply for a visa at a U.S. Embassy. Use of the electronic application form is thought to reduce processing time for visa applicants, ensuring that their visit to the Embassy or Consulate is as short and convenient as possible. Beginning 1st November 2006, applications submitted with a handwritten or typewriter typed DS-156 visa application form can no longer be accepted.

Applicants, who apply using a third-party contractor for remote data entry, and truly emergency cases, are exempt from this requirement.

The EVAF is available in several languages, and prints with a two-dimensional ("2-D") barcode that allows consular personnel to electronically scan more than 30 data fields into consular computer systems in a matter of seconds.

Since the EVAF was introduced in 2003, the amount of time saved on data entry has increased dramatically, allowing U.S. consular officials to attend to visa applicants far more rapidly than in the past. Though not previously mandatory, the EVAF is already used by nearly 70% of all applicants who apply for U.S. visas.

Applicants who appear for their visa interviews without a completed EVAF will experience delays in the processing of their application, but may be given the opportunity to complete the EVAF using an Internet computer at the Embassy or Consulate, or at a nearby public Internet facility, if available, in order to complete their application on the date of their scheduled appointment.

The EVAF will enable more rapid data sharing between the relevant competent authorities.

Privacy Concerns

- Which are the safeguards to protect the privacy of data of EVAF applicants?
- What is the delimitation of access of data by competent authorities and other bodies in the US?
- To what extent would this method exclude computer illiterate persons; persons with certain disabilities as well as persons with little or no access to Internet - this is a concern also of a number of EU citizens as well as persons from developing countries, from accessing a US non-immigrant visa?

Privacy and Civil Liberties Oversight Board in the US

The Intelligence Reform and Terrorism Prevention Act of 2004 established the Privacy and Civil Liberties Oversight Board in the United States. The Privacy Board consists of five members appointed by the President. The Board is part of the White House Office within the Executive Office of the President and supported by an Executive Director and staff.

The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. This includes advising on whether adequate guidelines, supervision, and oversight exist to protect these important legal rights of all Americans.[22]

Privacy Concerns

The board meets in secret and provides no public reports or analyses, and notably supported the President's domestic surveillance programme, which permits the interception of domestic communications of US citizens without judicial approval.[23] This board does not provide, according to its remit, supervision of privacy related to data of non-Americans.

Privacy experts have recommended stronger oversight mechanisms consistent with the recommendations of the 9-11 Commission Report.[24]

Now, lawmakers want to replace the White House privacy and civil liberties board created by Congress in 2004 with one that is more independent of the president.[25]

Senator Joseph I. Lieberman (I-Conn.), the chairman of the Homeland Security and Governmental Affairs Committee and Rep. Bennie Thompson (D-Miss.), chairman of the House Homeland Security Committee, have expressed concern that the Privacy Oversight Board has been largely ineffective.
Title VIII of the Implementing the 9/11 Commission Recommendations Act of 2007 would strengthen the Privacy Board by making it an independent agency, requiring Senate confirmation of all members, and establishing subpoena authority and reporting requirements.[26]
The measure passed the House of Representatives on January 9, 2007.
Similar legislation has passed in the Senate on March 13, 2007.[27]
However, it is possible that the President will veto the legislation because of a provision to grant agency employees limited collective bargaining rights.
The President has said that this would curb needed flexibility at the U.S. Transportation Security Administration and diminish traveller safety.[28]

[22] The White House, "Privacy and Civil Liberties Oversight Board," http://www.whitehouse.gov/privacyboard/
[23] "Oversight board briefed on NSA surveillance: Some impressed by 'how careful' the government is in protecting privacy," Associated Press, Nov. 28, 2006, http://www.msnbc.msn.com/id/15932976/
[24] Marc Rotenberg, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11," *Social Science Research Network Working Paper Series* (Sept. 2006), http://epic.org/epic/ssrn-id933690.pdf
[25] "Congress Seeks 'Bite' for Privacy Watchdog," *The Washington Post*, at D1, Feb. 13, 2007.
[26] The Library of Congress: Thomas, "H.R.1: Implementing the 9/11 Commission Recommendations Act of 2007 (Engrossed as Agreed to or Passed by House)," http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.+1:
[27] The Library of Congress: Thomas, "S.4: Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007 (Reported in Senate)," http://thomas.loc.gov/cgi-bin/query/D?c110:2:./temp/~c110m5X5Kq::
[28] "White House threatens to veto 9/11 bill," *Reuters*, Feb. 28, 2007.