European Union Center
Center for West European Studies
University of Pittsburgh

AVIATION SECURITY AND PASSENGER DATA EXCHANGE – THE NEED FOR A MULTILATERAL ARRANGEMENT

Dinos Stasinopoulos

and

Martin Staniland

Working Paper No. 6
May 2005

University Center for International Studies

EU Center/CWES website: **http://www.ucis.pitt.edu/cwes**
West European Studies Virtual Library website:
http://www.library.pitt.edu/subject_guides/westeuropean/wwwes/

AVIATION SECURITY AND PASSENGER DATA EXCHANGE – THE NEED FOR A MULTILATERAL ARRANGEMENT

Dinos Stasinopoulos - European Commission
Martin Staniland – University of Pittsburgh (1)

Summary

While this is a note about aviation security, it does not purport to be a comprehensive analysis of the sector. It seeks rather to highlight the US initiatives relating to airline passenger data exchange, outline EU responses to US measures and discuss the December 2003 Agreement to resolve the conflict arising from divergent legal systems on privacy and opposition by civil liberties groups (2). It then argues for a multilateral-global framework to provide legal certainty and achieve wider acceptance and consensus.

The events of September 11, 2001 have brought about new challenges to aviation security. In the rush to strengthen security and reduce the risks of future terrorist attacks, the United States has introduced a series of measures covering technical and economic aspects of both passenger and cargo aviation (3). These measures have generated an important debate about their impact on the privacy of passengers traveling to the US.

In order to improve aviation security, on November 19, 2001 the US adopted the Aviation and Transportation Security Act (ATSA). This Act requires airlines flying to the US to supply US Customs with information relating to passengers before take-off or at least 15 minutes after departure (4). On May 14, 2002, the US adopted another law requiring airlines to transfer passenger data to the US Immigration and Naturalization Service. In addition, through the Advanced Passenger Information System (APIS), the US agencies require the name, date of birth, nationality, sex, passport number, and any other information needed to identify passengers. Finally, the US also requires data collected from computer reservation systems (CRS), which are connected to the Passenger Name Record System (PNR)(5).

The above initiatives and other subsequent US measures such as CAPPS II have generated international debate about the impact of these measures on rights to privacy and highlighted the need for a proper balance between aviation security and privacy protection. The EU has insisted that compliance with US measures contravenes the existing national legislation of EU member states and in particular Article 25 of the EU Directive on the protection of personal data that prohibits the transfer of personal data from the EU to third countries that do not possess “adequate” data protection. The EU Directive on Data Protection is comprehensive privacy legislation. It came into effect on October 25, 1998 and requires the transfer of personal data only to non-EU countries that provide an "adequate" level of privacy protection (6). This legislation also requires the creation of government agencies and prior approval before data transfer may take place. The US approach to privacy combines legislation, regulation and industry self-regulation.

This long-running quarrel between the US and the EU over data exchange for transatlantic air passengers was finally concluded with an agreement signed in December 2003. The Agreement between the European Commission and the US Bureau of Customs and Border Protection broke a two-year negotiation deadlock and is a first step in the search for a balance between aviation security and data protection laws. More fundamentally, these long negotiations have highlighted important differences in data protection, which reflect cultural and legal differences about the role of government in regulating privacy (7). The EU and US share the goals of enhancing aviation security and privacy protection but differ over the means to achieve them. The Agreement was opposed by civil liberties groups on both sides of the Atlantic. In April 2004, the European Parliament voted to refer the Agreement to the European Court of Justice.

We are now witnessing a three-sided conflict over security and privacy, involving the European Commission, the European Parliament (EP) and US authorities, with the European airlines caught in the middle. The US side maintains that the agreement provides security and protects privacy for travelers. The Commission (which negotiated on behalf of the EU) and the Council (which approved the agreement) argued that civil liberties are sufficiently protected and that the EU has already won a number of concessions to protect privacy. The EP feels that the Commission and the Council have gone out of their way to avoid the Parliament's scrutiny. The agreement, MP's claim, should have been submitted to the EP under the "assent" procedure and not only for a simple non-binding opinion (8).

In order to deal comprehensively with the consequences of the US measures, the opposition of civil liberty groups and the fragmentation of various national efforts, the development of a multilateral arrangement should be considered as a way to join all the parties - including industry representatives and civil liberties groups - in an international framework. This may prove to be a much more cost-effective way of satisfactorily taking into account privacy concerns and enhancing global aviation security. The European Union intends to raise the issue at the International Civil Aviation Organization (ICAO).

The Issues

Since September 11, 2001, transport security has been pushed to the top of the EU and US agendas. US initiatives have changed forever the way that transport security is approached. Transport authorities and service providers have had to adjust traditional security measures to respond effectively to the new security risks. The EU has given its full support to the US initiatives and has made considerable efforts to contribute, bilaterally and multilaterally, to the much-needed enhancement of aviation security in a number of areas. Thanks to this co-operation, progress has been made and further work is underway to ensure legal certainty and to seek global solutions and universal implementation. Concerted efforts to strengthen aviation security sometimes appear to be weakened by the complexity and the multi-faceted nature of the issues. The most acrimonious discussions have centered on a conflict over the personal data details of passengers traveling to the US and thus is the subject of this note. The US authorities are

adamant that they need to see the data to help them identify potential terrorists in the wake of the September 11 attacks. EU concerns relate to a range of measures adopted to serve the shared objective of security, but whose broader effect on personal privacy needs to be seriously assessed to preserve the balance between civil liberties and security.

The EU feels that the transfer of data may violate its data protection laws since such data cannot be released without passenger consent and has tried to find a compromise between security requirements and respect of civic liberties.

US Actions

Congress created the Transportation Security Administration (TSA) in November 2001, thereby ending the decades-old system that allowed airlines to contract out airport security to private companies. In late 2001, Congress passed the Aviation and Transportation Security Act (ATSA), which created the Transportation Security Administration (TSA) as a unit of the Department of Transportation (DOT). This Act gave the TSA responsibility for screening air travelers. In late 2002, Congress passed the Homeland Security Act, which created the Department of Homeland Security (DHS) and transferred the TSA to the new DHS. One of TSA's first initiatives was to establish the Office of National Risk Assessment (ONRA). ONRA's mission is to develop and maintain risk assessment systems to detect terrorist threats. A new comprehensive approach was introduced involving, *inter alia*, measures requiring EU airlines to provide information on passengers traveling to the US, bailing-out airlines with financial difficulties, cockpit security, scanning luggage for explosives, training pilots and flight attendants, and measures dealing with cargo security.

As a result of US initiatives, airlines are faced with ever-increasing security challenges and new information requirements. A key issue for the industry is the requirement for personal information on travelers to the US. Immediately after September 11, the US unilaterally rendered mandatory the Advanced Passenger Information System (APIS) by threatening non-complying airlines with significant fines. APIS requires EU airlines to provide US Customs with personal data on US-bound passengers related to their religion and ethnicity and to the financing of their travel to the US; and to share this data among federal, state and local agencies for the purpose of ensuring national security.

The Enhanced Border Security and Visa Entry Reform Act rendered mandatory the Advanced Passenger Information System (APIS) and threatened non-complying airlines with significant fines if passenger manifest information on passengers traveling to and from the U.S. is not submitted. Air carriers are also required by law to submit to U.S. Customs passenger manifest information on both passengers and crew members (including names, dates of birth, citizenship and gender, and passport and visa information) before their arrival in the US and prior to departure (Passenger Name Records [PNR] Data). If information is incomplete or inaccurate, airlines face fines of $5,000 per person payable to US Customs and $1,000 per flight to the U.S. Immigration Service. Travel agencies in Europe feel that the current configuration of the Computer

Reservation Systems (CRSs) does not accommodate all data requirements. An interim new rule published in the June 25, 2002 Federal Register requires air carriers to grant the U.S. Customs Data Center electronic access to the carriers' automated reservation system and/or department control system that sets out the identity and travel plans of all passengers on flights in foreign air transportation either to or from the U.S. In order to boost compliance, the Customs Service has introduced additional provisions. Effective immediately, Customs will not approve new landing rights requests from carriers that do not give APIS data and will assess non-compliance fines up to $5,000. Also, the minimum standard for complete and accurate data will increase to 97 percent. Another issue is the double immigration checks (departure and arrival) to which passengers are being subjected, where the possibility of reciprocal arrangements has not been explored.

Before the terrorist attacks of September 11, the US airlines conducted travelers screening and administered the Computer Assisted Passenger Prescreening System (CAPPS I), subject to federal guidelines. ONRA was mandated by the Congress to implement the CAPPS II system - the new generation passenger-screening system - which is primarily designed to confirm the identities of air travelers and to identify travelers who may pose a security threat. It will use routine information from the CRSs to confirm a passenger's identity and assess the risk level. It should be noted that since September 11, in addition to PNR and APIS, there is other US legislation that seems to undermine civil liberties in the name of security (9).

The EU's Response to US Initiatives and the December 2003 Agreement

In the aftermath of September 11, the European Commission rushed to prepare legislation on improving air security, most notably in airports. On September 21, 2001, the European Council called on Member States to introduce more stringent security measures concerning technical training for crews, checking and monitoring of hold luggage, protection of cockpit access and quality control of security measures. New proposals have been put forward to support the aviation industry in areas such as insurance, unfair competition and financial compensation. New initiatives have also been launched to increase security and prevent terrorist acts. These measures were outlined in a Communication of October 2001 that specifically examined US initiatives and reviewed the state of play and measures taken by Member States. The Laeken Summit (December 2001) welcomed the adoption of a common position by the Council regarding the regulation of aviation security. On the international front, work is under way at the ICAO to establish a list of mandatory international security rules for domestic as well as international flights and to monitor compliance. These rules cover access to the cockpit, including strengthened doors, and remote surveillance of the cockpit.

The EU's cooperation with the US is based on the New Transatlantic Agenda (NTA) which shapes US-EU relations in aviation security (10). The NTA process is summit-driven and emphasizes joint action to address key issues such as emerging security challenges in the context of globalization. The 1998 Transatlantic Economic Partnership (TEP) produced "Guidelines on Regulatory Cooperation and Transparency"

that further encouraged both sides to exchange information and promote regulatory convergence. Thus a dialogue on aviation security was initiated within this framework and *ad hoc* expert groups created to tackle regulatory security issues. This co-operation was reinforced by the Transatlantic Legislators' Dialogue (TLD) and the involvement of the Congressional and EU legislators on regulatory policy issues such as privacy and data exchange. In 2003, Congressmen Mica and DeFazio and their colleagues in the European Parliament participated in a positive video conference on the conflict between EU privacy regulations and the US requirement to access airline passenger data to combat terrorism. In late 2002, the EU and the US began talks on the issue by attempting to strike a balance between data provision and aviation security. The EU has stressed the need for consultation with airlines to take into account their concerns over the practicality and benefits of the APIS and the conformity of APIS requirements to the EU data protection laws (11). In March 2003, the European Commission and US Customs and Border Protection (CBP) reached a transitional arrangement regarding the sharing of passenger data on transatlantic flights. Since then, EU airlines have been obliged to supply the CBP with Passenger Name Records (PNR) data for passengers whose travel itinerary includes flights into, out of, or through the US. In exchange for the agreement to release data, the CBP has given the EU assurances about the appropriate handling of this data. This agreement represents a transitional system and both sides agreed to work towards a bilateral arrangement under which the EU will adopt a legislative act in accordance with the provisions of EU data protection legislation.

Discussions continued throughout 2003 and in December the European Commission agreed to provide the US with Passenger Name Records (PNR) on its airline passengers traveling to the US, thereby ending a long-running battle between the EU and the US and removing a potential rift in transatlantic co-operation. This agreement covers only PNR and comes after a year of negotiations in which the US has sought extensive access to personal data of passengers traveling to the US (12).

The Commission produced a draft Decision (with 25 preambles and 8 articles) declaring that the "Undertakings" provided by the US for access to passenger record data (PNR) are "adequate" under EU law (Article 25.6 of the 1995 Data Protection Directive). The Decision included an "adequate finding" statement, affirming that US privacy protections to be implemented by the DHS are appropriate to guarantee air travelers' privacy. It also affirms that the protections put in place for the use, sharing, and monitoring of information, as well as the redress mechanisms associated with the use of data by the CBP, are sufficient under European law agencies as allowed by the agreement. The data will be retained for three and a half years for use by the CBP in fulfilling its own law enforcement functions and by other law enforcement agencies as allowed by the agreement.

The US, for its part, agreed to create an independent body outside the US government with the right to examine and correct data held by it. The agreement will enter into force and be in place for three and a half years, with renegotiations beginning in two and a half years. The DHS will initiate a series of undertakings related to how the DHS and the CBP will utilize and retain the PNR data and will put in place privacy

protections and redress mechanisms. The US also agreed to provide similar data on US citizens when they fly to Europe. In addition, the European Commission has committed itself to proceed with rapid negotiations about a legal framework for TSA's use of PNR data for CAPPS II.

According to the data protection office of Lufthansa, the December 2003 agreement has resulted in a so-called "push solution" to restrict the threat to European travelers' privacy. The push solution calls for airlines to create a back-up copy of travelers' information stored in their PNR (Passenger Name Record) system 24 hours before departure. This would allow airlines to filter sensitive information that is protected under the European Data Protection Directive. The information then would be transferred to CBP, instead of allowing full access to all data.

On March 29, 2004, the Agreement was adopted by the EU Ministers of Justice and Home Affairs. On April 1, 2004, the European Parliament voted by 229 to 202 in favor of the suspension of the agreement and reiterated its opposition to the transfer of passenger data to US authorities. On April 21, the EP voted to refer the agreement to the European Court of Justice. The MP's felt that there were legitimate reasons for requesting the Court to rule on both the procedure and the substance of the agreement on the ground that sharing passenger data with a foreign country violates European law. MEPs did not agree with the Commission that the US authorities provided enough privacy safeguards and called on the Commission to re-open negotiations. Furthermore, the vote calls into question the Commission's authority to negotiate international agreements on behalf of the EU. The vote also seems to indicate the MPs' desire to use the issue to expand their power in light of the ongoing discussions on the Constitution. In addition to these bilateral negotiations, the EU continued its efforts to bring the passenger data exchange issue up for discussion at the ICAO. The EU Working Party on Aviation has agreed on a submission to the next meeting of the ICAO for a global agreement on the prior transmission of passenger data (PNR) before a plane takes off. In addition to the US, Canada and Australia are introducing PNR schemes and law enforcement authorities around the world are increasingly requesting access to passenger data to deal with the threat of terrorism.

The Agreement and its Critics

The EU and US share the goals of enhancing aviation security and privacy protection but differ over the means to achieve them. These differences reflect divergent cultural and legal approaches to the role of government in regulating privacy (13). The EU/US Agreement on data passenger exchange has generated international debate on its impact on privacy rights and highlighted the need for a proper balance between aviation security and privacy protection. Civil liberties advocates in the EU have insisted that compliance with US measures contravenes the existing national legislation of EU member states and in particular Article 25 of the EU Directive on the protection of personal data that prohibits the transfer of personal data from the EU to third countries that do not possess 'adequate' data protection. The EU Directive on Data Protection is comprehensive

privacy legislation. It came into effect on October 25, 1998, and requires the transfer of personal data only to non-EU countries that provide an "adequate" level of privacy protection. This legislation also requires the creation of government agencies and prior approval before data transfer may take place.

The transfer of data to US agencies is not an obligation of the airlines according to EU law and can hardly be seen as relating to the original obligation of the airlines to their customers, which is to issue a ticket and deliver a service. This difficulty could be overcome and disclosure of data could be allowed if the airlines get the consent of their passengers. The Directive also prohibits any processing of sensitive data without explicit consent or substantial public interest. With regard to the transfer of data to third countries, Article 25 of the EU Directive defines an 'adequate level' of safeguards and permits data transfer for combatting terrorism.

A brief analysis of the main Articles of the EU Directive on Data Protection that imposes strict requirements on data collection and processing is provided below:

- Data processing must be allowed for an explicit and legitimate purpose (Article 6 [1b]);
- Data collection must be adequate, not excessive, and relevant to the purposes for which data are collected (Article 6 [1c]),
- Data must be accurate and must only be shared as long as it is necessary for the given purpose (Art. 6 [1d and e]).

There are also other obligations such as the right to know if data is being processed and for what purpose (Articles 10 and 11), as well as the right of access (Article 22).

National Security Exemption Clause

The Directive provides (Article 13) exemptions to the data processing obligations by stipulating that the scope of the obligations may be restricted when such restriction constitutes a necessary measure to safeguard national security and public safety. This requirement is a specific request with which the US general request does not comply.

Limits to Original Purpose

The US requests violate the general purpose of the Directive, which stipulates that data-processing is allowed only as long as it is compatible with the original purpose for which the data have been collected. The air carriers collect data in order to deliver a service and not to transfer data to the US. Furthermore, Article 6 cannot apply to transfer of data related to persons not traveling to the US.

Transfer of Data to "Third Countries"

The Directive prohibits any transfer of data to third countries if these countries do not provide an "adequate level" of protection and safeguards. Therefore, even if it is argued that the transfer is compatible with the contractual purpose of the air carriers (since without the transfer of data, the air carrier cannot carry passengers to the US), the consent of each individual passenger is required for the transfer. Other exemptions from the third country prohibition listed in Article 26 are not applicable since there is no proof that the transfer is necessary to safeguard public interests.

The Agreement has been criticized by civil liberty groups on both sides of the Atlantic for violating privacy rights. They claim that data privacy rights have been eroded in response to the Sept 11 events (14). Measures such as PNR and APIS concerning data retention would normally have taken years to debate but, post-September 11, they were pushed right to the top of the agenda and rushed through, despite opposition by personal liberties groups. These groups have stressed the need for consultations with airlines and civil society, so that the practicality and benefits of passenger data exchange and its conformity with legal frameworks can be taken into account. Despite US efforts to deal with the impact of these measures on civil liberties, privacy continues to be a marginal consideration in the development of US policy. Civil liberties advocates feel that such measures have diminished privacy protection in significant ways. It is now much easier for law enforcement officers to conduct surveillance and eliminate the checks and balances that previously were given to the courts to ensure that these powers are not abused.

Despite opposition from civil liberties groups, the European Commission has agreed to data transfers as it was felt that this was the only practical way of avoiding lengthy delays for European travelers to the US and fines against European airlines which do not provide the required data to the US authorities. The European Parliament felt that some of the information required by the US authorities is classified as sensitive in Europe and that, once stored in the US, there are no guarantees that it will not be shared or even transferred to third countries. EU citizens will have no effective right to access nor will they be able to correct the data. They cannot seek legal redress for its misuse and they will be subject to US administrative undertakings without commensurate rights under it. The agreement establishes a weak due process procedure that is entirely internal to the US Department of Homeland Security, whereas EU rules require a true right of redress for citizens who believe their data is being abused. Privacy International, for example, argued that the agreement has not assured adequate protection, clear purpose limitation and non-excessive data collection and does not guarantee against data transfer beyond the Department of Homeland Security (15).

With regard to following up on the December 2003 Agreement, there are several critical issues that concern the airlines and these need to be addressed. Steps must be taken to ensure that airlines are not forced to violate the laws of their own or other countries in order to comply with US requirements. Airlines are subject to their own national legislation and to the data protection laws of the countries in which they operate.

However, in most instances an airline's ability to comply with US requirements will be based upon political decisions taken by US authorities and other governments. This requires active cooperation between the US and appropriate ministries and data privacy authorities (where they have been established) in the various countries. Gaining final approval from various governments for providing US authorities with access to carriers' systems will likely prove to be a very complex and time-consuming process in many instances, particularly in those EU countries that have implemented data privacy laws in compliance with the 1995 EU Directive. A considerable challenge to EU-US relations is how to structure relations within the NTA process to deal with bilateral issues and how to move toward multi-lateralizing transatlantic arrangements for global consensus. In fact, security standards on which the EU and the US are in accordance are more likely to become accepted by other countries, thus becoming de facto international standards.

The EU also felt that the preparation of a single model at the global level is the most cost-effective way to combat terrorism and terrorism-related crimes with international implications. It is imperative to start work on a global framework to bring all interested stakeholders to the negotiating table and to develop a framework that takes into account aviation security and personal data protection requirements. This will help to avoid time-consuming bilateral talks and ensure coordination and convergence between the various systems worldwide.

In order to restore the public's confidence in the aviation system, personal information provided to airlines must be adequately protected within a global framework. For these reasons, the EU fully supports initiatives to create a multilateral framework for data transfer within the ICAO. The Commission believes that it is entirely impractical for all airlines collecting and processing data to have to operate under multiple unilaterally-imposed or bilaterally-agreed requirements. A paper submitted by the Netherlands on behalf of the Community and its Member States calls upon the ICAO to develop international standards to remove technical burdens that may impair the smooth functioning and implementation of those uniform practices, which could include the appropriate configuration of the PNR system. These globally-agreed standards are necessary to ensure harmonization of data exchange methodologies and processes. The 35th Session of the ICAO Assembly in 2004 decided to set up a working group to address a range of different aspects concerning categories of data, data processing requirements, data transfer requirements and data structure and to submit its report early in 2005 (16).

Conclusions

This analysis of the main elements of policy developments on privacy-related aviation security measures since September 11, 2001 permits a number of tentative conclusions about the possibilities for an effective resolution of the issue based on a global consensus. US aviation security measures on data transfer, which came into effect after September 11, 2001, have generated an important debate on their impact on the privacy protection of passengers traveling to the US. Privacy and aviation security are two major areas of concern on both sides of the Atlantic. However, approaches with

regard to the means of enhancing security vary between the EU and the US. Many European analysts believe that the impact of US measures on privacy will outweigh the improvement of security. Normally, such measures would have followed years of debate but, after September 11, they were pushed to the top of the agenda and rushed through despite opposition from civil liberties groups on both sides of the Atlantic. These groups have stressed the need for consultations with industry and civil society so that the practicality and benefits of the measures and their conformity with data protection requirements of the EU and other countries can be assessed and taken into account. A central issue in the debate lies in the possibility of using the information provided to the US authorities to serve purposes unrelated to the fight against terrorism.

Growing concerns over privacy in the US came into sharper focus in January 2004 as US lawyers pursued cases against Northwest Airlines in the US for handing over passenger data to the federal government. The suit seeks, *inter alia*, an order for Northwest to notify all passengers affected by the passenger data requirement. The airline has argued that, while believing it appropriate in the interest of aviation security to transfer data to the government, a protocol should be set up to address privacy concerns. As a result of these proceedings, US airlines have agreed to work with the DHS on traveler privacy protection.

At issue here is how the data will be treated. Will passengers be informed that personal information is being shared with the government? Will the rules be clear about the purposes for which data can be shared? Many industry analysts feel that it is necessary to develop internal protocols.

The December 2003 Agreement between the Commission and the US authorities can be considered as a first step towards an international solution to security issues such as the transfer of passenger data. It was seen by the Commission as the only practical way of avoiding lengthy delays for European travelers to the US and fines against any European airlines that did not provide data to the US authorities. The Agreement was approved by the European Council, while the European Parliament voted to refer it to the European Court of Justice. Member State governments have been asked to refrain from finalizing the agreement with the US until the Court has delivered its opinion on the compatibility of the data transfer with EU law. Divergent legal frameworks (US privacy law protects US citizens, while EU privacy law protects personal data in the EU) have provided the basis for the EP's opposition to the agreement and have prevented its final conclusion.

We are now witnessing a three-sided conflict over data protection involving the European Commission, the EP and US authorities, with the European airlines caught in the middle. The US maintains that the agreement provides security and protects privacy for travelers. The Commission (which negotiated on behalf of the EU) and the Council (which approved the agreement) argued that civil liberties are adequately protected and that the EU had already won a number of concessions to protect privacy. For example, US authorities will store the data for only 3 1/2 years instead of 50 years as originally requested. Of the approximately 60 data items originally requested, only 34 remain on the

list - mainly passenger name, address, date of ticket issuance, and number of pieces of baggage checked. The EP feels that the Commission and the Council have gone out of their way to avoid its scrutiny. It claims that the agreement should have been submitted to the EP under the "assent" procedure and not for a simple non-binding opinion (13). Some analysts in Europe feel that the EP hijacked the issues of aviation security and privacy for the sake of an inter-institutional power play with the Commission.

Although the agreement has helped to reduce differences about data protection, uncertainties remain between the EU and the US about the scope of privacy safeguards and the degree of legal certainty achieved with the agreement. It should be noted that the agreement covers only PNR and that the US is proceeding with further work for additional requirements that could complicate further the search for legal certainty.

The most pressing challenge is to promote aviation security at the global level by contributing to the development of a comprehensive regime that takes into account American and European concerns, as well as third countries' requirements, while providing additional legal certainty. The EU and the US must act in concert and play leading roles in this context.

Therefore, there is a need to develop an aviation security framework in the form of an international agreement that avoids the privacy protection pitfalls implied by the US approach, improves legal certainty and eliminates the need for bilateral negotiations that fragment efforts and result in conflicting compliance requirements for the affected airlines.

The European Community and its Member States intend to seek the development of uniform practices and standards at the international level within the framework of the ICAO. It is felt that ICAO standards would assist the industry to design their systems according to a standard model rather than being faced with different systems that would be bothersome and costly. The EU global initiative for an arrangement in the ICAO should be launched as soon as possible. To sum up, the development of a multilateral arrangement joining all the parties, including industry representatives and civil liberty groups, could prove to be a much more cost-effective way of enhancing global aviation security and coordinating fragmented national efforts.

Endnotes

(1) Dinos Stasinopoulos, a former European Commission official, would like to thank Professor Alberta Sbragia, Director of the Center for West European Studies (CWES) and the European Union Center (EUC), and the Center's staff for their support during his Fellowship at the University of Pittsburgh. This note was prepared as a part of an EU Fellowship research project carried out in fall 2002 at the EUC of the University Center for International Studies. Martin Staniland is Professor in the Graduate School of Public and International Affairs, University of Pittsburgh.

(2) Definitions of privacy vary widely according to context. This note interprets privacy in terms of data protection and management of personal information; see J. Michael, "Privacy and Human Rights" (UNESCO 1994) and W. J. Long and M. Pang Qeek M., "Personal Data Privacy Protection in an Age of Globalization," *Journal of European Public Policy* 9:3, 325-344.

(3) Some of these proposals, such as cockpit security, baggage screening, and placing sky marshals in flights, are sound security measures and do not implicate privacy interests. They are therefore not dealt with here.

(4) On November 19, 2001, the US President signed the Aviation and Transportation Security Act (ATSA), which among other things established the TSA within the Department of Transportation. TSA's main function is to implement the Act by reforming the nation's transport security system. The Act established a series of challenging but critically important milestones toward achieving a secure transport system. More broadly, however, the Act will fundamentally change the way transportation security will be managed in the US. The Act recognizes the importance of security for all forms of transportation and related infrastructure elements. Infrastructure protection of critical assets such as airports and more than 10,000 FAA facilities is another of the TSA's key missions. Along with airports, other transportation networks are critical to U.S. economic and national security and vital for the free and seamless movement of passengers and goods throughout the country.

(5) PNR refers to processing data held in airline reservation systems as a tool for enhanced risk assessment applied to flights arriving from international ports of embarkation. This is a separate undertaking and should not be confused with Advanced Passenger Information (API) regimes.

(6) The main legal instrument for data protection is the Data Protection Directive 95/46/EC of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on free movement of such data (*OJL* 11.23.1995). However, delays in implementation by Member States and differences in the ways the directive has been applied at the national level have caused problems that are particularly due to the lack of clarity of some transposition laws. Efforts are being made to achieve clarity and to simplify procedures and notification requirements.

(7) As early as 1990, discussions were held to iron out differences and to provide a streamlined means for compliance, and the US and the European Commission developed a "safe harbor" framework. The Safe Harbor arrangement on privacy and data protection is a hybrid, quasi-formal or informal arrangement and represents a compromise between the EU approach of formal, legal governance of privacy and the US approach that relies on self-regulation and creates a legislative interface between the two approaches. It includes the following seven principles:

(a) Notice - An organization must inform individuals about the purposes for which it collects information about them;

(b) Choice - An organization must offer individuals the opportunity to choose whether, and how, personal information they provide is used or disclosed to third parties;

(c) Transfer - An organization may disclose personal information to third parties consistent with the principles of notice and choice;

(d) Security - Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss or unauthorized access;

(e) Data Integrity - Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered;

(f) Access - Individuals must have reasonable access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate; and

(g) Enforcement - Effective privacy protection must include mechanisms for assuring compliance with safe harbor principles, recourse for individuals to whom the data relate to ensure compliance with the principles, and punitive consequences for the organization when the principles are not followed.

(8) The assent procedure was introduced by the Single European Act (1986). It means that the Council has to obtain the European Parliament's assent before certain very important decisions are taken. Parliament can accept or reject a proposal but cannot amend it.

(9) The "USA Patriot Act" - no. 107-56/2001 - requires agencies to consider both security and privacy as they implement regulations on a range of security measures and identify policy alternatives that would achieve the same security goal while limiting the impact on privacy. The "Federal Agency Protection of Privacy Act" aims at establishing basic checks and balances on federal agencies' decisions to use and disclose personal information. The Act would require agencies to engage in a systematic review of privacy before federal regulations are adopted and would encourage enhanced public participation and agency accountability for individual privacy interests.

(10) In addition to the NTA process, transatlantic relations in transportation security are embedded in a dense network of multilateral links, including annual meetings of the Group of Eight (G8), semi-annual meetings among top officials, and shared partnership in international organizations such as the ICAO and the European Civil Aviation Conference (ECAC). The international institutional environment within which the US and EU cooperate in addressing aviation security is also of crucial importance because most of the issues have a global dimension. International organizations regularly contribute to the establishment of rules and norms (regimes) regulating international activities such as aviation, maritime transportation and customs. The roles played by the ICAO and the ECAC in aviation security are illustrative of the value and importance of regimes. This partnership at the multilateral/plurilateral level is supplemented by the bilateral framework of the New Transatlantic Agenda (NTA) that shapes US-EU relations in aviation security.

(11) "Communication from the Commission to the Council and the Parliament on Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach."

(12) "Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection." (*Official Journal of the European Union*, L. 183/83, 5.20.2004).

(13) Four models of information protection have been developed worldwide: (a) comprehensive laws; (b) sectoral laws; (c) industry self-regulation; and (d) privacy-enhancing technologies. Legal frameworks on the collection, processing and disclosure of personal information have been the object of different approaches on both sides of the Atlantic. The EU has developed comprehensive data-protection legislation, while the US relies on a combination of sectoral laws, self-regulation, and privacy-enhancing technologies for data protection. There is no explicit guarantee of privacy rights under the Constitution of the US since no equivalent federal data privacy legislation exists. The fundamental problem is that there are no clear legal remedies for breaches of data privacy. The US approach has been to set up industry-specific codes of practice that provide a measure of protection, although there are no substantive penalties for non-compliance and these codes are not considered by the EU as offering an adequate level of protection. The US, however, does not legislate *a priori* and relies on the Courts to effectively sanction a deficit in data protection. The EU gives priority to the protection of personal data an *a priori* basis through legislation and it defines privacy as a human right, while the US tends to trust the private sector and the market to protect personal privacy. The EU law, in particular the EU Directive that provides strict safeguards on the use and disclosure of data, has spurred the development of comprehensive data protection around the world.

(14) C. Laurent, "Data Protection since 11 September 2001: What Strategy for Europe?" Statement at the European Parliament's Public Seminar, March 25, 2003, Brussels.

(15) Privacy International "Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection" (2004).

(16) An International Framework for the Transfer of Airline Passenger Data (Passenger Name Record-PNR) to Public Authorities. This working paper submitted to the ICAO recommends that the ICAO work address the following issues concerning data:

(a) *Categories of data* - The maximum number and scope of data that is strictly necessary for law enforcement purposes and enhancing aviation security should be considered. The list of data to be considered should be proportionate and not excessive;

(b) *Data processing requirements* - Transparency, purpose limitation, storage of data, rights of passengers, safeguards and redress mechanisms should be considered;

(c) *Data transfer requirements* - Type of access, time of transfer, filtering and security measures should be considered;

(d) *Data structure* - Various options for harmonizing or modifying the current structure of PNR should be assessed.

Dinos Stasinopoulos, formerly with the European Commission's Directorate General for Energy and Transport, served in the Commission for over 20 years. His responsibilities were quite diverse including developing and representing Community positions on energy and transport in the ECMT, the UN, and the WTO; as well as developing cooperative relationships in those sectors with Russia and the U.S. In the fall 2002, Mr. Stasinopoulos served as the European Union Fellow at the EU Center at the University of Pittsburgh. He has published various articles on the development of the EU's policy and integration in the transport and energy sectors.

Martin Staniland, Professor and International Affairs Division Director at the Graduate School of Public and International Affairs at the University of Pittsburgh, specializes in international relations, especially trade in services including transportation; and European Union politics and economic issues. He has written books on West African politics, theories of political economy, and American interpretations of African nationalism. He has the following titles in press: *Government Birds: The State and Air Transport in Western Europe* (Rowman and Littlefield) and "Competition versus competitiveness in the European single aviation market," in Miriam L. Campanella and Sylvester C.W. Eijffinger, eds., *EU Economic Governance and Globalization* (Edward Elgar).

The views expressed in this paper are purely those of the authors and may not be regarded as stating an official position of the institutions for which the author is or has been working. All views expressed are personal and should not be regarded as the European Union Center's or Center for West European Studies' position on the issues covered in the paper. The European Union Center (EUC) and the Center for West European Studies (CWES) are housed within the University Center for International Studies (UCIS) at the University of Pittsburgh, and are the publishers of the Policy and Working Paper Series. Approximately two papers are published annually.

The Policy and Working Paper Series are funded by a generous grant from the European Commission and by a separate grant from the US Department of Education's Title VI grant program for National Resource Centers for Area Studies. The papers are distributed free of charge to US scholars and students specializing in Western Europe, as well as to members of the business, diplomatic, and legal communities, the media, and other interested specialists. All papers are available on the EUC/CWES website.

Inquiries about this series and manuscripts for review should be submitted to:
Center for West European Studies
4200 Wesley W. Posvar Hall
University of Pittsburgh
Pittsburgh, PA 15260, USA
Tel: (412) 648-7405
Fax: (412) 648-2199
E-mail: **cwes+@pitt.edu**