Istituto Affari Internazionali

IAI WORKING PAPERS 12 | 06 – March 2012

Building the Transatlantic Area of Freedom, Security and Justice. The Case of the Passenger Name Record Agreements

Andrew Byrne

Abstract

For years, controversy has plagued the EU's attempts to agree on a legal basis for sharing the personal details of airline passengers with the US. Now, opposition in the European Parliament may see this form of counter-terrorism cooperation rejected. The arguments are about more than record-keeping: they relate to the need to assure passenger security in the post-9/11 era but also the risk that these security practices can pose to the privacy and personal liberty of normal citizens. This paper analyses the development of EU-US PNR data-sharing agreements as a case study for wider transatlantic security cooperation. Reviewing the key challenges from the PNR story presents a strong argument for the US to fully engage with the EU on "internal" security measures that can assure transatlantic security externally. To fully maximize the opportunities however, agreements like PNR need independent oversight and redress procedures. Without such elements, failure on PNR is more likely and the possibilities for a wider transatlantic area of freedom, security and justice may narrow.

Keywords: *European Union / United States / EU-US security cooperation / Aviation security / Passenger Data Collection / Passenger Name Record (PNR) Agreement*

Building the Transatlantic Area of Freedom, Security and Justice. The Case of the Passenger Name Record Agreements

by Andrew Byrne*

Introduction

Over two years after the Lisbon Treaty was ratified familiar complaints rumble on: that the EU's attempts at conducting a common foreign policy through the European External Action Service have been an embarrassment, that the Libya crisis has exposed the Common Security and Defence Policy (CSDP) as irrelevant and that, from a US perspective, the EU has little to offer in security terms. For many in Washington, the EU appears to be at best an exercise in managing tensions in the European backyard, at worst a sclerotic organization, which threatens global economic stability.

Yet the EU has quietly been conducting productive transatlantic cooperation on important security matters, most recently through the latest Passenger Name Record (PNR) Agreement. Indeed, cooperation on Freedom, Security and Justice (FSJ) is providing the most fruitful return on transatlantic security cooperation. The PNR Agreement demonstrates that the EU is the natural interlocutor for the US on important FSJ issues that can boost security and resilience.

This paper analyses the development of EU-US PNR data-sharing agreements as a case study for wider transatlantic security cooperation. Reviewing the key challenges from the PNR story presents a strong argument for the US to fully engage with the EU on "internal" security measures that can assure transatlantic security externally. However, the paper argues that in order for this effort to bear fruit, three lessons must be borne in mind:

- Firstly, security cooperation increasingly risks materializing at the expense of liberties; criticism of this trade-off is rising. Hence, greater oversight of the use of PNR and improved redress processes for injured parties would increase legitimacy, build popular support for such cooperation more generally and will also audit effectiveness. This can be done without undermining national security prerogatives.

- Secondly, political leadership and practical engagement channels are necessary to make cooperation of this kind workable. The early signs are not promising however. Both the US and the EU stand to lose much if efforts to provide high-level political guidance to cooperation and appropriate practical channels of exchange (both congressional and diplomatic) do not emerge.

Paper prepared for the Istituto Affari Internazionali (IAI), March 2012.

* Andrew Byrne is a Marie Curie PhD Fellow on EU external relations. He was Research Assistant at the Istituto Affari Internazionali (IAI) from November 2011 to March 2012 in the framework of the EU-wide training programme EXACT.

- Finally, aviation security is but one element of what should be a wider Transatlantic FSJ agenda. Constant technological development and vigilance is necessary to ward off threats in the sky but terrorists are increasingly looking to strike in areas where they have an asymmetric advantage: The new frontiers in homeland security lie beyond aviation and the EU has an important contribution to make in building resilience to shared threats.

1. Background

Two years ago on Christmas Day, Umar Farouk Abdulmutallab boarded a flight from Amsterdam to Detroit. As the plane began to descend over Michigan, Abdulmutallab slipped into the airplane toilet, washed himself, brushed his teeth, and then returned to his seat to inject a syringe of chemicals into the bomb hidden in his underwear. Minutes later, he detonated the bomb, which cabin crew thought was a firecracker. The explosion failed to injure anyone except Abdulmutallab, but it undermined faith in the notion that a decade of aviation security upgrades and passenger data collection procedures had made terror in the skies a thing of the past.

Modern states are faced with difficult choices when seeking to protect their citizens' security: between increasingly sophisticated and interconnected systems of personal data collection and an absolute commitment to the privacy of a citizen's personal data. When it comes to sharing the fruits of data collection with international partners, there exists a fundamental tension between an increasingly networked world - which is ideal terrain for terrorism - and the legal and political barriers to responsible sharing of citizens' data.[1]

Among the initiatives launched after 9/11 by the newly created Department of Homeland Security (DHS) was the collection of vast amounts of data on air passengers in order to screen and detect suspicious patterns of behaviour, enabling them to thwart terrorists like Abdulmutallab. Since 2001, DHS has required airlines to transmit all details they hold on passengers flying to the US, before the plane has landed. PNR (Passenger Name Record) data was to be a new tool in the effort to defend America's borders from terrorism: far less extreme than measures to detain and interrogate terror suspects, but still controversial because it subjects millions of civilians to detailed surveillance, even though they are not suspected of any criminal behaviour.

The problems with PNR have been legal, political and practical: it has taken the EU and the US almost ten years to agree on a durable legal basis for the current data transfers. Opposition from politicians and NGOs in Europe has been forceful. Even with a fully-fledged PNR-sharing system in operation, individuals like Abdulmutallab - already known to the US as a terror suspect - have been allowed to book tickets under their real names, board planes and undertake attacks despite a system designed to detect exactly such behaviour.

[1] Richard J. Aldrich, "Transatlantic Intelligence and Security Cooperation", in *International Affairs*, Vol. 80, No. 4 (July 2004), p. 732.

Notwithstanding, DHS officials claim that PNR has been crucial in thwarting potentially devastating attacks. Official secrecy on the details of terrorist monitoring and arrests makes comprehensive analysis of the effectiveness of PNR as a tool extremely difficult. However, reaching agreement on a legal basis for PNR exchange has been a priority for both sides for years, indicating that this is one surveillance tool that is of significant value: *"PNR data is a critical asset not just to secure the travel of U.S. citizens, but to provide for the safety and security of travelers from Europe and the rest of the world."*[2]

But how can we truly assess the effectiveness of PNR systems? How can we ensure it operates without undermining the civil liberties of European citizens? And how can we make sure that the EU and the US fully exploit the opportunities for productive and responsible security cooperation beyond PNR?

2. What is PNR?

PNR data includes all data registered by airline companies or travel agencies when a traveler makes a booking: the name of the person, seat number, travelling route, booking agent, credit card payment details, IP address, physical address, phone numbers etc.[3] The draft PNR Agreement between the EU and the US foresees 19 of these data elements for all travelers being automatically "pushed" to the US Department of Homeland Security within minutes of travel but this practice has been normal procedure since 2001, under bilateral arrangements with EU member states and subsequently under time-limited EU agreements from 2004 and 2007 onwards. For airlines with servers based in the US, the transfer can occur under US law.

What distinguishes PNR agreements from other forms of data sharing is that firstly all individuals, regardless of whether they have had any interaction with police authorities or not, have their data recorded, and secondly, the data is more detailed than standard passport information exchanged through the US's Advanced Passenger Information (API) system. Assuming full functionality of the US PNR system on all domestic and international flights to or within the US, over 800 million PNR identities must be processed by DHS each year.[4]

PNR data can be used in three ways:[5]
1. Reactively: After a crime has been committed, PNR can be used to investigate criminals and unravel criminal networks.

[2] Ambassador William Kennard comments, quoted in "EU unveils passenger data sharing proposals", in *EurActiv*, 23 September 2010, http://www.euractiv.com/en/transport/eu-unveils-passenger-data-sharing-proposals-news-497999.
[3] Evelien Brouwer, "The EU Passenger Name Record System and Human Rights: Transferring passenger data or passenger freedom?", in *CEPS Working Document*, No. 320 (September 2009), p. 3, http://www.ceps.eu/ceps/download/1976.
[4] Estimates from the Research and Innovation Technology Administration at the Bureau of Transportation Statistics, US Dept. of Transportation (http://www.rita.dot.gov).
[5] Timothy Kirkhope, *Draft Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime* (PE 480.855v01-00), 14 February 2012, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-480.855%2b01%2bDOC%2bPDF%2bV0%2f%2fEN.

2. In real-time: Prior to the arrival or departure of passengers, the data can be used to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases, PNR data is especially useful for running passenger data against predetermined assessment criteria in order to identify persons that were previously "unknown" to law enforcement authorities but may pose a risk, based on their associations or patterns of behavior.

In real time, PNR data can also be matched against other databases with the data of those suspected of criminal offences or those who have been flagged as potential risks. This makes it possible to identify suspects and their associates well in advance of their travel to or from a country.

3. Pro-actively: The criteria for "suspicious behaviour" can be constantly developed and updated through analysis of PNR so that authorities can learn more about early warnings or suspicious behaviour.

Technology now allows these data activities to be carried out on a larger scale, and on an automated basis. It also allows this data to be shared with a much wider group of actors: everyone from the US Terrorist Screening Center (TSC) to local law enforcement officers. Crucially, the value of PNR data can be multiplied when it is cross-checked against any of the many other domestic databases. Problems also multiply, however, when data is stored in different forms across a multitude of databases, managed by different institutional actors and agencies.

The US Federal Bureau of Investigation (FBI) maintains a master database of watchlists and automatic selectee lists known as the "Consolidated Terrorist Screening Database" (TSDB) at the TSC. The database contained a total of 1 million records on 400,000 individuals by 2008. From this, the Transportation Security Administration (TSA) creates subsets of "no fly" and "automatic selectee" lists which are transmitted to frontline border agencies to compare with the PNR and API data of passengers to detect suspicious persons before they board a plane. PNR data are also run against at least 6 other databases on everything from drug smugglers to border entry registers to further profile minor crime suspects.[6]

3. EU-US agreements on PNR

Efforts to establish a permanent legal basis for the automated transfer of PNR data on passengers from the EU to the US have faced several hurdles to implementation over the last ten years. In 2006, the European Court of Justice (ECJ) annulled the 2004 Council Decision on the transfer of PNR data to the US, ruling that the agreement was not founded on an appropriate legal basis.[7] Following much high-level engagement,

[6] William J. Krouse and Bart Elias, "Terrorist Watchlist Checks and Air Passenger Prescreening", in *CRS Report for Congress*, No. RL33645 (30 December 2009), http://www.fas.org/sgp/crs/homesec/RL33645.pdf.
[7] Judgment of the European Court of Justice (Grand Chamber) of 30 May 2006 *European Parliament v Council of the European Union* (Joined Cases C-317/04 and C-318/04), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF.

including an address by US Homeland Security Secretary Michael Chertoff to the European Parliament, the Council subsequently approved a new agreement on a different legal basis in 2007, which is currently in effect, pending the new draft agreement.

Current attempts to ratify a new PNR Agreement with the US foundered in 2010 when the European Parliament (EP) used its newly acquired powers under the Lisbon Treaty to postpone its vote for consent for conclusion of this agreement. Proponents, including Home Affairs Commissioner Cecilia Malmström, say that the new draft agreement concluded in November 2011 to replace the 2007 Agreement includes a number of amendments to address civil liberties concerns.[8]

The Agreement is still pending approval from the EP, which is in doubt since the Civil Liberties Committee rapporteur, Sophie in 't Veld MEP, has recommended withholding consent.[9] The Agreement will likely go to a vote at a plenary session of the EP next spring and its approval will rest on whether the Socialists and Liberal Democrats group decide to support it.

According to some, the US has been able to impose the conditions in the agreement under which data is to be transferred without compromising on any points of concern.[10] The possibility that the alternative to a common agreement may be a patchwork of bilateral treaties between the US and individual member states, giving unequal levels of protection to European citizens' data, has undermined the bargaining power of the Commission and the EP vis-à-vis Washington.[11] While the Commission claims that the new draft agreement is an improvement on that which preceded it - opponents counter that substantial concerns have been ignored.

Should an EU-US agreement come into effect and the EU PNR System established, a large number of similar agreements are likely to be signed with other countries.[12] Should the EP fail to approve the agreement, MEPs have acknowledged that PNR data transfers will continue, most likely under bilateral agreements with member states. Without these agreements, European airlines would be open to legal action in the US for failing to share PNR with the US government and in a worst case scenario would be denied entry to the US.

4. Opposition to PNR sharing

The array of opponents to the Agreement on the basis of civil liberties concerns consists of actors in the EP - the liberal democratic bloc (ALDE), the Greens-European

[8] Commission press release *EU proposal for passenger data to fight serious crime and terrorism* (IP/11/120), Brussels, 2 February 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/120.
[9] Comments of Sophie in 't Veld MEP, at a hearing of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, February 2012.
[10] Ibidem.
[11] Interviews with Commission officials, February 2012.
[12] South Africa and the United Arab Emirates have already requested agreements. A more restricted PNR agreement has been concluded between the EU and Australia.

Free Alliance and the United and Nordic Left (GUE/NGL) - NGOs such as European Data Rights and also official agencies such as the European Data Protection Supervisor and the Fundamental Rights Agency, both of which have published opinions stating that the agreement violates the privacy rights of citizens without demonstrating necessity or proportionality.[13] In the Council, several member states also held reservations about the way in which citizens' data would be processed.[14]

This is not the first occasion in which initiatives in transatlantic internal security have run up against liberties concerns. In 2010, the EP struck down an agreement to share SWIFT banking data with the US as part of its terrorist financing and tracking program (TFTP).[15] When SWIFT, the Brussels-based company operating most financial transactions all over the world, moved its servers to Europe, a basis had to be found for the transfer of data that was compatible with EU law. For six months, DHS was unable to access important interbank data without subpoenas due to the EP's refusal to consent to the agreement. This was an early demonstration of the EP's willingness to flex its muscles in vetoing an international agreement (as recalled above, this is a power it gained under the Lisbon Treaty). More importantly for our purposes, it demonstrated that the counter-terrorism methods that governments employ increasingly involve the collection of vast amounts of personal and sensitive data which is passed on to the US.

In both the SWIFT and PNR cases, the central concern was how DHS would use the private data of citizens who are in principle not subject to any investigation. The major concerns on PNR relate to:

- The number of data elements transferred: according to some, the greater the number of data elements, the greater the potential for misidentification and wrongful interference with a passenger.[16]

- The length of time for which the data is stored: the current draft foresees the data being kept for fifteen years. Although the draft foresees data being "anonymized" after a shorter period, this is a reversible process.

[13] European Union Agency for Fundamental Rights, *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM (2011) 32)* (FRA Opinion-1/2011), Vienna, 14 June 2011, http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-June2011.pdf. European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Brussels, 25 March 2011, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-03-25_PNR_EN.pdf.

[14] Interview with Commission Official, Brussels. February 2012.

[15] Stanley Pignal, "European parliament rejects US data swap deal", in *Financial Times*, 11 February 2010, http://www.ft.com/intl/cms/s/0/6aa82fa8-170e-11df-afcf-00144feab49a.html.

[16] Elspeth Guild, "Oral evidence 21 March 2007", in 21st Report of Session 2006-07 of the House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL Paper 108), London, 5 June 2007, p. 32, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf.

- The access of other law enforcement actors to the data: whereas the 2007 Agreement listed specific agencies which could access the data, the new agreement contains no restricted list and thus could be said to be a regression in civil liberties terms.[17]

- The potential for religious or ethnic profiling using the data: this could be done indirectly through profiling dietary preferences, general airline comments or comparison with other databases.

- Export of the data by the US to third countries.

- Vagueness in the description of the kind of crimes for which PNR data could be used to prosecute: the threshold is set at crimes carrying an imprisonment sentence of three years or more, which amounts to an extremely broad category.

- The lack of access to meaningful judicial redress for passengers who feel they have been wrongfully treated on the basis of PNR analysis.

- Oversight and review of the conduct of PNR sharing: there are essentially no enforcement procedures for the terms of the agreement although a joint review can be carried out at its conclusion.

5. Principles of data protection

The conflict between security and privacy is a familiar problem in Western societies, as law enforcement agencies have traditionally advocated restrictions on the rights of ordinary citizens to increase their ability to identify potential offenders and prevent crimes. Yet legal systems set specific criteria defining what kinds of liberties can be restricted, in what ways, for how long and in what specific circumstances. Above all else, liberal democracies require security measures to be overseen by independent authorities (usually the courts) that can provide an avenue for redress for wronged parties. While the concerns laid out by opponents to PNR are much wider than oversight and redress (the list above is merely a summary), these final two points are the foundation of citizen protection, for without them, guarantees on the other points can be neither verified nor enforced.

Furthermore, under European data regulation since 1995, independent oversight of data use has been the cornerstone of the data privacy rights regime.[18] This principle has also been firmly established in the jurisprudence of the ECJ.[19] In the absence of any federal regime, the US system of data protection for individuals is clearly not

[17] Interview with Commission officials, Brussels, February 2012.
[18] See Directive 95/46/EC and Regulation (EC) No 45/2001 for specific details on the duties and powers of the European Data Protection Supervisor and the Assistant Supervisor, as well as the institutional independence of the supervisory authority.
[19] See European Court of Justice, Judgment of the Court (Grand Chamber) of 9 March 2010 *Commission v. Germany* (Case C-518/07), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0518:EN:NOT.

equivalent to that in the EU, particularly given the absence of any provisions for external, independent oversight on PNR data.[20] The US employs a 'sectoral' approach to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather than uniform federal regulations. The detailed and lengthy negotiations on PNR between the EU and the US are a reflection of this asymmetry. The core problem remains guaranteeing "adequate standards of protection" for data on EU citizens - the overarching principle in the 1995 Data Protection Directive.[21]

5.1. Transparency and oversight

Although there is no external oversight of the use of DHS's handling of PNR data, we already know from reports by the department's Privacy Office (which is in charge of overseeing its use of PNR data) that DHS has failed to account for its use of personal data as required by law. In 2006 the DHS Privacy Office report found that TSA had not accurately described its use of personal data as part of its screening programmes, required under the Privacy Act. [22]

5.2. Wrongful detention and redress

DHS has been prone to errors in issuing no-fly orders or detaining suspects based on PNR data - notably detaining Senator Ted Kennedy when airport security flagged him as a risk. The US-based American Civil Liberties Union (ACLU) has filed a class action against DHS on behalf of US citizens who believe they have been falsely detained on the basis of PNR data compared with other databases.[23] ACLU could do so under the terms of the Privacy Act. However, the act's provisions do not apply to European citizens and they have no avenues for redress through US courts.

When PNR is used to detail passengers wrongfully, the procedures for redress appear to exist on paper only. DHS reviews complaints from passengers regarding no-fly orders and watch lists using the Traveller Redress Inquiry Program (TRIP). A 2009 investigation by the US DHS Inspector General, Richard Skinner, into this redress system found that: *"Redress-seekers generally do not benefit from their participation in TRIP. Their cases often languish for extended periods and are handled inconsistently. Sometimes their cases are not brought to the attention of the appropriate agency. In other instances, cases are closed before all indicated agencies have had a chance to review them. Even when cases are properly reviewed, they do not usually produce meaningful results for redress-seekers."*[24]

The report also found that in some cases, where aggrieved passengers were able to have their names added to a "cleared travel" list, these lists were either not transmitted

[20] Peter Carey, *Data Protection. A Practical Guide to UK and EU Law*, 3rd ed.,Oxford, Oxford University Press, 2009.
[21] Ibidem.
[22] William J. Krouse and Bart Elias, "Terrorist Watchlist Checks and Air Passenger Prescreening", cit.
[23] Rahman v. Chertoff, Case No. 05 C 3761, filed June 19, 2006, http://www.aclu-il.org/news/press/rahman%20amended%20complaint%20--%20final.
[24] Dept of Homeland Security, *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program*, Report conducted by US DHS Inspector General, Richard Skinner, 11 September 2009, p. 107, http://www.oig.dhs.gov/assets/Mgmt/OIG-09-103r_Sep09.pdf.

to airlines or, when they were, they sometimes were misinterpreted as secondary no-fly lists which meant that the passengers were subject to additional security measures.[25]

In light of this hardly optimal record, it is not surprising that EU-US PNR Agreements have been so controversial. On the major points of independent oversight and effective redress procedures, it is difficult to see how US concessions would undermine the privacy imperatives of this security activity, significantly increase costs, or hinder the ability of the US to make full use of PNR data in keeping with the content of the Agreement.

Establishing an independent oversight body that provides full guarantees of secure and confidential oversight of how PNR data is used would present additional advantages. One problem deriving from opaque data processing is that official secrecy is sometimes used as a veil to conceal bureaucratic errors. These errors can result in privacy violations but they can also allow terrorists to slip through the net. If oversight were undertaken on a fully independent, security-cleared basis, such transparency could help bring institutional shortcomings to light, providing a valuable effectiveness audit of current operations.

Doubtless, opponents would still complain of excessive data retention periods among other complaints, but conciliation on oversight and redress may yet prove to be the last great opportunity to secure a durable and politically acceptable deal at EU-US level.

6. Why everyone loses without an EU-US PNR agreement

Should the EP reject the Agreement next spring, there will most likely be no renegotiation of the deal between the Commission and DHS and a legal basis will be found for PNR data exchange through bilateral deals with member states.[26] This would be a bad outcome for everyone involved.

For the US, the costs are reputational and practical. Much has been done to improve perceptions of the US's counter-terror policies under President Barack Obama. However, the failure to agree proper rights standards for travellers to the US combined with the persistence of the Guantanamo Bay detention facility and the recent provisions for indefinite detention of terror suspects in the National Defence Authorization Act 2012 would further the idea that little of substance has changed from the Bush era counter-terror strategy.

Practically, the US would be forced to negotiate twenty-seven bilateral agreements, each with differing provisions and qualifications, leading to a massively increased regulatory burden for an already overburdened DHS. If evidence were needed that DHS is already struggling to manage the processing of hundreds of millions of PNR records each year under essentially one regulatory code, then we might return to the case of Abdulmutallab. In this case, the bomber was not flagged as a risk under the

[25] Ibidem, p. 56-57.
[26] Comments by European Commissioner for Home Affairs Cecilia Malmström to Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, February 2011.

PNR system because DHS failed to effectively manage four separate databases[27] across five separate bodies with responsibility in this area.[28] The US Department of Justice found in an audit that these databases had significant difficulties and had not been completely audited to ensure records were complete and accurate.[29] Managing the US system for detecting terrorists travelling by plane is already a multi-agency bureaucratic nightmare, which is why an agreement for uniform PNR standards for all EU-US passengers is in the US's interest.

For the airline industry, a patchwork outcome means additional costs and a greater regulatory burden. European Commission estimates put the total cost for airlines of a standardized EU-US PNR data "Push" system at 24 million euro in set-up costs and 30 million euro in annual recurring costs. The costs under a patchwork scenario are certain to be exponentially higher.[30] It is worth bearing in mind that this is an industry already under major financial strain with notable US carriers filing for bankruptcy in 2011.[31]

Finally, the same problems apply for European governments: aside from another lengthy negotiation process, the costs of bilateral arrangements are likely to push the direct set-up costs to member state governments from approximately 60 million euro to well over 220 million euro.[32] This does not include recurring maintenance costs. This is mainly because each member state would have to establish its own Passenger Information Unit rather than establishing a centralized unit funded under the EU budget. For their citizens, a patchwork outcome would mean unequal levels of data protection depending on country of origin.

For all major stakeholders, an EU-US PNR Agreement is the optimal outcome in terms of costs, regulatory burden, effectiveness and rights equality. This in itself is an important lesson for transatlantic cooperation in security matters. As has happened in almost all initiatives at boosting internal and border security in the last ten years - the Mutual Legal Assistance and Extradition treaties, Europol data sharing, the Container Security Initiative (CSI), visa waiver and travel document agreements and the Terrorist Financing and Tracking Program - the US has come to appreciate that the advantages of engaging on an EU-US level far outweigh the negotiation costs. In most of these cases, the US - either by design or by accident - began by engaging with member

[27] The Consolidated Terrorist Screening Database (TSDB), the Terrorist Identities Datasmart Environment (TIDE) and Customs and Border Protection's (CBP) "No Fly" and "Automatic Selectee" lists.
[28] The National Counter Terrorism Center (NCTC), the Terrorist Screening Center (TSC), TSA, CBP and FBI. See William J. Krouse and Bart Elias, "Terrorist Watchlist Checks and Air Passenger Prescreening", cit.
[29] US Dept of Justice, *Review of Terrorist Screening Center* (Audit report 05-27), June 2005, p. 160, http://www.justice.gov/oig/reports/FBI/a0527/final.pdf.
[30] European Commission Staff Working Paper on *Impact Assessment, Accompanying Document To The Proposal For A European Parliament And Council Directive On The Use Of Passenger Name Record Data For The Prevention, Detection, Investigation And Prosecution Of Terrorist Offences And Serious Crime {Com(2011) 32 Final} {Sec(2011) 133 Final}* (SEC(2011) 132 final), Brussels, 2 February 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010SC0132:EN:NOT.
[31] Kyle Peterson and Matt Daily, "American Airlines and its parent company AMR Corp filed for Chapter 11 Bankruptcy in the US in November 2011", in *Reuters*, 29 November 2011, http://www.reuters.com/article/2011/11/30/us-americanairlines-idUSTRE7AS0T220111130.
[32] European Commission Staff Working Paper on *Impact Assessment*, cit.

states bilaterally. Either through legal requirements or by pragmatic argumentation, the EU successfully reshaped the negotiation forum and asserted its prerogative to negotiate on behalf of all member states on FSJ matters.[33] In the unlikely, but possible, event that the EP rejects the PNR Agreement in spring, the US should reflect once more on what significant concessions it can give on PNR that would not undermine any of its primary security objectives. External oversight by an independent authority and functional redress procedures appear to be low-cost solutions.

7. Political leadership and practical engagement - the necessary ingredients

In the long history of EU-US PNR Agreements, progress was made first of all when the US recognized that interests were best served by seeking agreement at EU-US level, rather than bilaterally with member states. The second ingredient for success was high-level political leadership and lobbying of actors in the EP. Since the 2010 debacle, the White House has become aware that the really significant foreign policy changes brought by the Lisbon Treaty lie in the provisions for FSJ cooperation and the EP's new power over international agreements.[34] In this vein, engagement by cabinet-level actors with the EP can help address European concerns and also provides impetus to actors within the US bureaucracy to prioritize cooperation. Likewise, Congress has an important role to play by interacting with the EP through working groups and regular dialogue.

In addition to building the political coalition for initiatives and setting the tone for engagement, leadership by US actors such as the Secretary of Homeland Security can build awareness among departmental units of the importance of investing effort in transatlantic FSJ efforts. Unfortunately, staffing and knowledge levels in some US institutional quarters are not optimal: the US Mission to the EU, for instance, no longer has any resident DHS official to deal directly with internal security matters in Brussels.[35] This is not a positive sign and the lesson from PNR is that FSJ efforts will falter without concerted engagement with all relevant actors.

8. Moving beyond aviation security

Constant technological development and vigilance is necessary to ward off threats in aviation and border security. The latest efforts focus on greater detection capabilities for chemicals and explosive gels and also for an agreement for scanning of all US-bound maritime cargo.[36] In line with this, efforts are being made to continually improve intelligence-sharing channels between DHS and the European Commission on a case-by-case basis.

[33] John D. Occhipinti, "Partner or Pushover? EU Relations with the US on Internal Security", in Daniel S. Hamilton (ed.), *Shoulder to Shoulder: Forging a Strategic US-EU Partnership*, Washington, Center for Transatlantic Relations at Johns Hopkins University, 2010, p. 121-139, http://transatlantic.sais-jhu.edu/publications/books/shoulder-to-shoulder-book-finaltext.pdf.
[34] Interview with official at the US Department of State, Washington, March 2011.
[35] Correspondence with Mission, February 2012. The last resident DHS Official returned to Washington in 2011.
[36] Interviews with Commission Officials, Brussels, February 2010.

However, aviation security is but one element of what must be a wider FSJ agenda. DHS must focus on how to manage the data it collects responsibly and effectively - a major challenge given its tendency to collect more and more information. The case of Abdulmutallab and numerous internal audits have exposed the problems DHS has in managing a comprehensive traveller surveillance system. Further increasing the range of data surveillance without adequate facilities to process data responsibly will likely lead to more embarrassing and time-consuming mistakes - distractions from other major security threats.

For the EU's part, it is engaged in a game of catch-up with US aviation security. Although work is ongoing, the EU still does not have the facilities to analyse and share PNR data on flights between member states. This is highly ironic given that the data protection barriers between member states can only be lower than those between the EU and the US - since 1995 there has been a common European area of data protection standards.

An improved PNR data collection and management system would better safeguard EU citizens' privacy while protecting their security. At the same time, however, an effective PNR system combined with the full range of aviation security measures currently in use and in development will push terrorists to search for other, less controlled, avenues to conduct their criminal acts. In the future, terrorists will likely strike in areas where they have an asymmetric advantage: arguably, this no longer lies in plane hijacking or exploding. The new frontiers in homeland security lie beyond aviation. Threats have proliferated in a highly interconnected and globalized transatlantic area. The arteries of the transatlantic system of trade, energy, communication and transportation exchanges are increasingly vulnerable to shocks in one area, which can provoke major disruption to the broader system. The range of threats to this network is also opaque and difficult to predict - arising from small groups of nebulous and mobile actors as well as global health and environmental hazards.

In this context of shared vulnerability, there is a major need for the EU and US to build resilience to multifarious threats: disruption to shipping routes, energy and communications infrastructure, cyber security, global health dangers and natural disasters.[37] All of these vulnerabilities call for a state of preparedness which scholars increasingly acknowledge can only come from shared contingency planning, early-warning systems, the proliferation of back-up systems and vulnerability audits.[38] In these areas, the EU is the natural interlocutor for the US, not only because of the reasons stated above but also because the EU is the pre-eminent actor for member states to coordinate their internal security responses. Attempts have begun with the creation of the EU-US working group on cyber-security, which is engaged in joint

[37] For a detailed discussion of these issues: Jeremy Walker and Melinda Cooper, "Genealogies of Resilience: From Systems Ecology to the Political economy of Crisis Adaptation", in *Security Dialogue*, Vol. 42, No. 2 (April 2011), p. 143-160. Filippa Lentzos and Nikolas Rose, "Governing Insecurity: contingency planning, protection, resilience", in *Economy and Society*, Vol. 38, No. 2 (May 2009), p. 230-254.

[38] Daniel Hamilton and Mark Rhinard, "All for one, one for all: towards a transatlantic solidarity pledge", in *Chaillot Papers*, No. 127 (30 December 2011), p. 67-76, http://www.iss.europa.eu/publications/detail/article/the-eu-us-security-and-justice-agenda-in-action.

readiness exercises.[39] Progress in this area should illustrate the benefits for broadening such exercises.

Conclusions

In addition to the observation that the EU is the most effective actor for the US to engage with on important matters of freedom, security and justice, the PNR process presents three lessons for wider transatlantic security cooperation:

- The first lesson revolves around ***liberty***. Security cooperation will increasingly come at the risk of diluting liberties and actors criticizing security cooperation on this basis will become increasingly vocal. Openness with data in the use of PNR, independent oversight and improved redress processes for injured parties would help build legitimacy and would also audit the effectiveness of such measures more generally. The US stands to gain much more from genuine engagement with the EP on civil liberties matters than it would by pursuing alternative bilateral arrangements.

- The second lesson relates to ***politics***. There is now awareness in Washington that engagement with the EP needs to be upgraded to maximize the gains from EU-US cooperation. The political momentum for PNR Agreements grew at key moments when key figures from the administration and Congress alike met with EP leaders and actively took part in the dialogue on EU US cooperation.[40] Leadership must come from the top levels of the executive, be matched with initiatives in Congress and be reflected at bureaucratic level if the US wants to move ahead with Europe to build a transatlantic area of freedom, security and justice.

- The third and final lesson concerns ***resilience***. Aviation security is but one element of what should be a wider FSJ agenda. Constant technological development and vigilance is necessary to ward off threats in this area but terrorists will look to strike in areas where they have an asymmetric advantage. The new frontiers in homeland security lie beyond aviation and if the EU and the US are successful in learning the lessons from the PNR experience and tackling these threats together, they stand a good chance of shaping the global architecture of resilience in the twenty-first century.

Updated: 15 March 2012

[39] Ibidem. This Working Group - formalized by President Obama in the US-EU Summit Declaration of 20 November 2011 - provides for the continued sharing of cybersecurity best practices and security standards and enhances collaboration on public-private partnerships, cyber incident management, and combating cyber crime).
[40] Secretaries Clinton, Chertoff and House Speaker Pelosi all met with figures from the EP to further EU US security cooperation.

References

Books and articles

Richard J. Aldrich, "Transatlantic Intelligence and Security Cooperation", in *International Affairs*, Vol. 80, No. 4 (July 2004), p. 731-753.

Evelien Brouwer, "The EU Passenger Name Record System and Human Rights: Transferring passenger data or passenger freedom?", in *CEPS Working Document*, No. 320 (September 2009), p. 3, http://www.ceps.eu/ceps/download/1976.

Evelien Brouwer, *Towards A European PNR System? Questions on the Added Value and the Protection of Fundamental Rights*, Study prepared for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), January 2009, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=30170.

Peter Carey, *Data Protection. A Practical Guide to UK and EU Law*, 3rd ed.,Oxford, Oxford University Press, 2009.

Mary De Rosa, "Privacy in the age of terror", in *The Washington Quarterly*, Vol. 26, No. 3 (Summer 2003), p. 27-41, http://www.twq.com/03summer/docs/03summer_derosa.pdf.

Elspeth Guild and Evelien Brouwer, "The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US", in *CEPS Policy Brief*, No. 109 (July 2006), http://www.ceps.eu/book/political-life-data-ecj-decision-pnr-agreement-between-eu-and-us.

Daniel Hamilton and Mark Rhinard, "All for one, one for all: towards a transatlantic solidarity pledge", in *Chaillot Papers*, No. 127 (30 December 2011), p. 67-76, http://www.iss.europa.eu/publications/detail/article/the-eu-us-security-and-justice-agenda-in-action.

William J. Krouse and Bart Elias, "Terrorist Watchlist Checks and Air Passenger Prescreening", in *CRS Report for Congress*, No. RL33645 (30 December 2009), http://www.fas.org/sgp/crs/homesec/RL33645.pdf.

Filippa Lentzos and Nikolas Rose, "Governing Insecurity: contingency planning, protection, resilience", in *Economy and Society*, Vol. 38, No. 2 (May 2009), p. 230-254.

Michael Levi and David S. Wall, "Technologies, Security, and Privacy in the Post--9/11 European Information Society", in *Journal of Law And Society*, Vol. 31, No. 2 (June 2004), p. 194-220.

Valsamis Mitsilegas, "The New EU–USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data", in *European Foreign Affairs Review*, Vol. 8, No. 4 (Winter 2003), p. 515-536.

John D. Occhipinti, "Partner or Pushover? EU Relations with the US on Internal Security", in Daniel S. Hamilton (ed.), *Shoulder to Shoulder: Forging a Strategic US-EU Partnership*, Washington, Center for Transatlantic Relations at Johns Hopkins University, 2010, p. 121-139, http://transatlantic.sais-jhu.edu/publications/books/shoulder-to-shoulder-book-finaltext.pdf.

Patryk Pawlak (ed.), "The EU-US Security and Justice Agenda in Action", in *Chaillot Papers*, No. 127 (30 December 2011), http://www.iss.europa.eu/publications/detail/article/the-eu-us-security-and-justice-agenda-in-action.

Jeremy Walker and Melinda Cooper, "Genealogies of Resilience: From Systems Ecology to the Political economy of Crisis Adaptation", in *Security Dialogue*, Vol. 42, No. 2 (April 2011), p. 143-160.

Documents

Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) [Official Journal L 204/18 of 4.8.2007], http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=4401

European Commission, *Commission Staff Working Paper: Impact Assessment, Accompanying Document To The Proposal For A European Parliament And Council Directive On The Use Of Passenger Name Record Data For The Prevention, Detection, Investigation And Prosecution Of Terrorist Offences And Serious Crime {Com(2011) 32 Final} {Sec(2011) 133 Final}* (SEC(2011) 132 final), Brussels, 2 February 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010SC0132:EN:NOT

European Court of Justice (Grand Chamber), Judgment of 30 May 2006 *European Parliament v Council of the European Union* (Joined Cases C-317/04 and C-318/04), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF.

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. Brussels, March 2011. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-03-25_PNR_EN.pdf

European Parliament Committee on Civil Liberties, Justice and Home Affairs, *Draft Recommendation on the draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security* (PE480.773v01-00), 1 February 2012, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/890/890797/890797en.pdf

European Union, *European Commission adopts an EU external strategy on Passenger Name Record (PNR)* (IP/10/1150), 21 September 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1150

European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [Official Journal L 281 of 23.11.1995], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

European Union, *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data* [Official Journal L 8 of 12.1.2001], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:NOT

European Union Agency for Fundamental Rights, *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM (2011) 32)* (FRA Opinion-1/2011), Vienna, 14 June 2011, http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-June2011.pdf.

UK House of Lords European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement*, 21st Report of Session 2006-07(HL Paper 108), London, 5 June 2007, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf.

UK House of Lords European Union Committee, *The United Kingdom opt-in to the Passenger Name Record Directive*, 11th Report of Session 2010-11 (HL Paper 113), London, 11 March 2011, http://www.publications.parliament.uk/pa/ld201011/ldselect/ldeucom/113/113.pdf.

US Dept of Homeland Security, *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program*, Report conducted by US DHS Inspector General, Richard Skinner, 11 September 2009, p. 107, http://www.oig.dhs.gov/assets/Mgmt/OIG-09-103r_Sep09.pdf

US Dept of Homeland Security, *Fact Sheet: DHS's International Engagement*, 2 December 2011, http://www.dhs.gov/ynews/fact-sheets/20111202-dhs-international-engagement.shtm

US Dept of Homeland Security, *How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel*, Testimony of David Heyman, Assistant Secretary, Office of Policy, before United States House of Reprsentatives-Committee on Homeland Security-Subcommittee on Counterterrorism And Intelligence, Washington, 5 October 2011, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20DHS_0.pdf

US Dept of Homeland Security, *Secretary Chertoff's Remarks to European Parliament*, Brussels, 14 May 2007, http://useu.usmission.gov/may1407_chertoff_ep.html

Latest IAI Working Papers

12 | 05 N. Van Raemdonck, Vested Interest or Moral Indecisiveness? Explaining the EU's Silence on the US Targeted Killing Policy in Pakistan

12 | 04 E. Oğurlu, Rising Tensions in the Eastern Mediterranean: Implications for Turkish Foreign Policy

12 | 03 F. Zwagemakers, The EU's Conditionality Policy: A New Strategy to Achieve Compliance

12 | 02 E. Soltanov, The South East Europe Pipeline: Greater Benefit for a Greater Number of Actors

12 | 01 N.Sartori, The European Commission's Policy Towards the Southern Gas Corridor: Between National Interests and Economic Fundamentals

11 | 30 D. Sammut, After Kazan, a Defining Moment for the OSCE Minsk Process

11 | 29 F. Ismailzade, The Nagorno-Karabakh Conflict: Current Trends and Future Scenarios

11 | 28 A. Dessì, Algeria at the Crossroads, Between Continuity and Change

11 | 27 R. Alcaro and A. Dessì, The September UN Vote on Palestine: Will the EU Be Up to the Challenge?

11 | 26 F. Di Camillo and V. Miranda, Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward

11 | 25 N. Mikhelidze, The 2012 Presidential Elections in Russia: What Future for the Medvedev-Putin Tandem?

11 | 24 S. Felician, North and South Korea: A Frozen Conflict on the Verge of Unfreezing?

Istituto Affari Internazionali
Via Angelo Brunetti, 9 00186 Roma
Tel.: +39/06/3224360 Fax: + 39/06/3224363
E-mail: **iai@iai.it** - website: **http://www.iai.it**
Send orders to: **iai_library@iai.it**

The Institute

The Istituto Affari Internazionali (IAI), founded by Altiero Spinelli in 1965, does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations.
The IAI publishes an English-language quarterly (The International Spectator), an online webzine (AffarInternazionali), two series of research papers (IAI Quaderni and IAI Research Papers) and an Italian foreign policy yearbook (La politica estera dell'Italia).