CENTRE FOR EUROPEAN POLICY STUDIES
Thinking CEPS ahead for Europe since 1983

Tracing Terrorists: The EU-Canada Agreement in PNR Matters

CEPS Special Report/September 2008

Revised version 17.11.2008

Peter Hobbing

Abstract

Enhancing border security in support of the global 'war against terrorism' is very much in vogue these days, in particular as regards the control of air passengers. Seven years after 9/11, this trend is yet unbroken. While the build-up of defences occurs in most cases at the one-sided expense of civil liberties, the EU-Canada Agreement of 2005 is different: quite justly, it holds the reputation of a well-balanced instrument respecting the interests of citizens. Still, instead of serving as a model for future instruments, the Agreement rather runs the risk of being scrapped at the next possible occasion. A close look at the passenger name record (PNR) 'mainstream', as embodied by the EU-US branch of transatlantic relations with four Agreements rapidly succeeding between 2004 and 2008, reveals the opposite tendency away from data protection and towards an unconditional tightening of controls.

This report undertakes to examine the doubtful benefits of such an approach by assessing the price to pay inter alia for 'false positive' mismatches and other collateral damages, while the actual achievement of a higher degree of public security remains very much in the dark, mostly owing to the impossibility of making all borders 100% secure. As a result, no critical reason emerges for taking leave of the good practices established by the EU-Canada instrument.

This work was prepared as part of the EU–Canada project – *The Changing Landscape of Justice and Home Affairs Cooperation in the European Union and EU–Canada Relations* – funded by the European Commission, Directorate-General for External Relations, Relations with the US and Canada.

This project assesses the relations between the European Union (EU) and Canada in the area of Justice and Home Affairs (JHA). It aims at facilitating a better understanding of the concepts, nature, implications and future prospects related to the Europeanization of JHA in the EU, as well as its role and dilemmas in the context of EU–Canada relations.

ISBN-13: 978-92-9079-809-5
Available for free downloading from the CEPS website (http://www.ceps.eu)
© Peter Hobbing, 2008

Unless otherwise indicated, the views expressed are attributable only to the author in a personal capacity and not to any institution with which he is associated. This publication may be reproduced or transmitted in any form for non-profit purposes only and on condition that the source is fully acknowledged.

Contents

TRACING TERRORISTS: THE EU-CANADA AGREEMENT IN PNR MATTERS

CEPS Special Report/September 2008

PETER HOBBING*

We just want to fly.[1]

Introduction

The uproar is frequent at Heathrow Airport and elsewhere. Over and over again, there are new security measures addressing new threats: we have become accustomed to baggage prohibitions of all kinds in terms of scissors, miniature knives and bottled liquids. We have become used to standing in endless queues waiting for security checks before boarding a transatlantic plane – or just transiting at an intermediary stop under the constant threat of missing a connection.

While excessive queues and similar obstructions are felt as a direct assault on our personal freedom, we normally show much more patience towards intrusions into our privacy. 'Simple' transmissions of airline passenger data to security services go widely unnoticed and it is mainly privacy commissioners and other civil liberties watchdogs who complain. It is a different story, though, when these intrusions are combined with significant travel delays as in the case of electronic travel authorisation schemes that are about to come into vogue. "Why announce travel intentions 72 hours in advance?" upset passengers start asking, as they wonder how the inflation of security measures relates to global mobility, 'open skies' and other liberal concepts that currently dominate the headlines.

Maybe it is the price we have to pay for being able to travel within hours from one end of the world to the other or maybe it is attributable to the growing sense of insecurity we encounter after 9/11 especially in air travel. Maybe there are other reasonable explanations of why such obvious restrictions to our sphere of personal freedom and integrity are unavoidable.

Data processing even where done for high-ranking security purposes is not a game without rules, however. It is subject to international standards as developed by the OECD and transposed into national law by the various member countries. The present report undertakes to check the extent to which the criteria in question have been respected by the legislators. Although such scrutiny – in view of the interests at stake – may not require any special justification, the reader may well question why we examine these vital issues on the basis of the 2005 EU–Canada Agreement, which is undoubtedly the least-contested international instrument in the field. The point is well taken, given that all arrangements involving the US provide for much more explosive content and for conflict between governments on the one side and privacy commissioners/civil liberties groups on the other.

Still, we believe that EU–Canada relations on the matter of the passenger name record (PNR) present a highly valuable research topic providing clues to all the strategies and tools available in

---

* Peter Hobbing is Senior Associate Fellow at CEPS and a former Principal Administrator at the European Commission.

[1] A passenger's sigh in view of new security measures at airports as reported by journalist Josef Joffe (Joffe, 2007).

airline security. On the one hand, the current EU–Canada Agreement stands out from the rest by its measured and legally balanced approach, which left it practically unchallenged from the usual criticism and gave it the nimbus of a model instrument. On the other hand, the 2005 Agreement is not for eternity: due to its sunset clause it will expire in 2009 if not positively reconfirmed in negotiations starting this summer. With the current 'climate change' and a wind definitely blowing in favour of tightened security, there are continued tendencies to cut back privacy standards. The main indicators are the recent EU border package of February 2008 with a number of discomforting features that seem to be taken right out of the US toolbox in border security; on the Canadian side, civil liberty activists are dismayed by the new 'no flight' legislation adopted last year. And beyond, there is still the US in its role of a looming giant setting the pace in global border control: if the US invites the Eastern European EU member states to join the visa waiver programme (VWP) at the price of abandoning established EU PNR standards, one must be aware that the winds of change might also affect the forthcoming EU–Canada negotiations.

It would seem all the more important that we take the opportunity to review the situation, underlining the advantages of the current arrangements and stressing the possible dangers of trying to turn back the wheel of time.

This report proceeds in three steps, more specifically 1) retracing the metamorphosis of PNR airline data from a commercial facilitation device to a widely recognised tool of counter-terrorism; 2) analysing the extent to which the current use of this tool is acceptable, especially in terms of privacy protection; and 3) determining the practical benefits obtained from its use.

1. Tip of the iceberg: PNR functions within air transport, flight security and border surveillance

Airline history is that of the fastest growing transport industry: its advance from the first powered flight (by the Wright brothers in 1903) to the first commercial passenger flight took just 11 years.[2] Charles Lindbergh's transatlantic solo flight of 1927 was soon followed by commercial airlines crossing the Atlantic, at first via South America and Africa, with the riskier northern route not becoming standard until the start of World War II in 1939[3] (see Box 1).

Box 1. Interwar developments

In Europe as well as North America, internal services expanded considerably in the interwar years: with the first European airline taking up service in February 1919 (Deutsche Luft-Reederei GmbH, Berlin–Weimar), there were 28 mainly national airlines operating in European skies by 1939 (Mulder, 2005).

In the early 1930s, Canada was one of the few industrialised countries without a national airline. It was only in 1937 that the newly founded Trans-Canada Airlines started to provide air service linking the Atlantic and Pacific oceans (CBC, 2004).

In the US, the number of air passengers rose between 1932 and 1938 from 474,000 to 1.2 million, but still represented no more than a meagre 7.6% of the long-distance train market. At the time, flying was still considered a privilege "limited mostly to the upper class" (US Centennial of Flight Commission, 2003).

[2] See the article "Airline" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Airline).

[3] See the article "Transatlantic flight" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Transatlantic_flight).

The real airline boom occurred worldwide after World War II, when traffic increased by double-digit rates practically every year between 1945 and 1970, while the total number of annual passengers skyrocketed from 9 million to 311 million (ICAO, 1970). After some slowdown in the 1970s owing to the first oil crisis, the pace accelerated again thanks to technical innovation and, most of all, deregulation and privatisation of carriers, reaching 1.2 billion passengers in 1992 (IATA, 2007). The boom was also mirrored in the success of the transatlantic routes: rising steadily, the annual passenger volume between the EU and US reached 50 million in 2007, thus becoming the largest international air-transport market by far. And its size is expected to expand by another 50%, thanks to the recent EU–US open skies agreement (EurActiv, 2007; European Commission, 2008). Similar negotiations are underway, under the heading of 'blue skies', between the EU and Canada – equally a market with a clear upward trend.[4]

It is quite evident that the management of such a volume of traffic requires an enormous degree of streamlining in order to cope with the mass of passengers. While in the 1930s cooperation among airlines in organising networks and performing a correct repartition of airfares in case of multi-sector trips (revenue allocation) relied on more or less hand-knitted formulas, by 1960 the airline industry had to take advantage of modern information technology to ensure smooth travel operations in a widening market.

The PNR system thus developed proved to be a handy formula to cast essential data elements on individual travellers into a concise format that could easily be exchanged not only among airlines but also among other organisations linked to the system. It was therefore no surprise that law enforcement agencies – following the rise of aircraft hijacking in the 1970s and 1980s – started to show a vivid interest in accessing the data that had been gathered on airline passengers. Despite the insistence with which security services have pursued their goal, one should not overestimate the importance of PNR data as an isolated element. What counts is the overall scenario of data sources available: only their painstaking matching with data from other sources such as crime or terrorism databases will lead to reliable results.

1.1 From open skies to electronic borders: The versatile role of the PNR in civil aviation

With respect to passenger data, airline history can be subdivided into roughly three phases: 1) the pre-electronic 'pioneer' age; 2) advanced technology for travel facilitation purposes; and 3) post-9/11, dual exploitation for travel and security purposes.

1.1.1 PNR as an instrument of travel facilitation

In the 'stone ages' of flying, the greatest achievement in travel booking (and important advantage over the railways as the main competitor) was seen in the fact that it could be done by telephone and later by telex. All the rest remained rather old-fashioned: tickets for multi-leg flights "consisted of a long series of paper coupons that detailed every leg of the trip" (US Centennial of Flight Commission, 2003). Airline staff would mark the reservation on a card and file it. As demand for air travel increased and schedules grew more complex, this process became impractical.[5]

---

[4] This underlines the fact that the Canada–EU air market is 'large and mature'. In 2006, with more than 6.7 million one-way passenger trips, the EU was Canada's second largest bilateral air market after the US (Transport Canada, 2007).

[5] See the article "Computer reservations systems" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Computer_reservations_system).

In 1946, the era of automated booking started with the electromechanical Reservisor installed by American Airlines, while tests commissioned by Trans-Canada Airlines in 1953 investigated a computer-based system with remote terminals. But it took until 1959 to set up the first modern **computer reservation system (CRS), SABRE**,[6] which was able to conduct reservation storage and retrieval operations as well as transactions involving the services provided by various carriers.[7]

Besides the CRS, initially created and run by the airlines themselves, there are now large **global distribution systems (GDSs)** that book and sell tickets for multiple airlines. They are typically used for bookings by travel agents or even travellers by means of travel websites (Internet gateways). There are currently the following four GDSs: Amadeus, Galileo, SABRE and Worldspan, whereby Amadeus is the only Europe-based one, with the others being located in the US.[8]

When bookings are made by airlines, travel agents or travellers, the first step is to create a file containing the following five items: 1) the name of the passenger(s); 2) contact details for the travel agent of the airline office; 3) ticketing details – either a ticket number or a ticketing time limit; 4) the itinerary of at least one sector, which must be the same for all passengers listed; and 5) the name of the person making the booking.

The **PNR** thus created and complemented by a unique, alpha-numeric record locator represents the centrepiece of the travel operation. Just like an interlocking puzzle, further elements may be attached to it such as additional itinerary 'legs', and even hotel and car reservations. If passengers require flight services provided by different airlines in order to reach their destination ('interlining'), reservation information in the form of copies of the original 'master' PNR will be transmitted to the other airlines and stored in their respective CRS/GDS.[9]

While the abovementioned five PNR elements are considered the minimum, there is a considerable amount of other information mostly required by the airlines and the travel agent to ensure efficient travel. These include,

- fare details and any restrictions that may apply to the ticket;
- the form of payment used, as this will usually restrict any refund if the ticket is not used;
- further contact details, such as telephone contact numbers at a home address and intended destination;
- age details if relevant to the travel, e.g. unaccompanied children or elderly passengers requiring assistance;
- frequent flyer data;
- special service requests (SSRs) such as special meal requirements, seating preferences and other similar requests; and
- other special instructions (OSIs), comments that are passed on to ground staff to enable them to assist passengers.[10]

---

[6] See the article "Semi-Automatic Business Research Environment" (ibid.).

[7] Ibid.

[8] Ibid.

[9] See the article "Passenger Name Record" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Passenger_Name_Record).

[10] Ibid.; for further details see also the sample PNRs from the SABRE and Galileo GDS in appendix II.

Designed to "facilitate easy global sharing of PNR data", the CRS/GDS companies "function both as data warehouses and data aggregators, and have a relationship to travel data analogous to that of credit bureaus to financial data" (EPIC, 2006, p. 81). As the list of data items is just as evolutionary as the number of commercial branches such as hotels, car rental firms or others wanting to process their transactions by means of the GDS, it is no surprise that the PNR also arouses the interest of government agencies that look at flight operations from an entirely different angle.

1.1.2 Post-9/11 developments and its precedents

Airplanes in the air have always been a sensitive security issue: since the first days of flying, intelligence services have anticipated the risk of **espionage** carried out by foreign reconnaissance aircraft.[11] Even airline passengers aboard commercial airplanes could be suspected as potential spies, which may explain why nowadays they are still sometimes subject to photo interdiction at least when passing over military installations/strategic locations.

In a second phase, the threat turned against the airplane and its passengers when **hijackers** took hostages to exercise pressure on airlines/governments in an effort to extort transportation to a given location, to hold the hostages for ransom or to achieve political and publicity goals, e.g. the release of comrades being held in prison. Hijacking operations were mostly linked to major political struggles such as the US–Cuban conflict in the 1950s and 1960s, the Palestinian–Israeli conflict, separatist movements in Asia and militant underground groups in Europe (e.g. the hijacking of the Landshut Lufthansa plane by the Rote Armee Fraktion in 1977).[12]

In a third phase, the **in-flight destruction of aircraft** as well as the killing of passengers became the direct objective of the assailants: although the 1988 Lockerbie crash with 259 dead (attributed to Libyan terrorists) remains the most widely known incident, numerous attacks of a similar kind came before and afterwards.[13]

The landmark events of the 9/11 suicide attacks were finally characterised by a further escalation: in addition to annihilating the plane and passengers, the terrorists used the fuelled aircraft as a **guided missile to destroy ground targets**, the final aim being to sow fear and terror in the Western world rather than pursue a concrete political purpose.

Beyond the technique of the terror assault, 9/11 also represented a **landmark in terms of responses to the threat of hijacking**: reactions resulted first in a number of technical measures to address the specific risks that had emerged during the events.

Before 9/11, the recommended response was for the crew inside the airplane to obey the hijackers' demands so as to safeguard the passengers and buy time; since then the policy has

---

[11] As early as the balloon age, right after the French Revolution in 1789, the French army used the reconnaissance balloon l'Entreprenant to identify Austrian troop movements in the battle of Fleurus (1794). See the article "Surveillance aircraft" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Surveillance_aircraft).

[12] For further examples, see the article "List of aircraft hijackings" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/List_of_notable_aircraft_hijackings).

[13] See the article "History of Terror Attacks" in History Central (online) (retrieved from http://www.multied.com/Terrorhistory.html).

been to prevent access to the cockpit and pilots. At check-in, air passengers worldwide are prohibited from carrying anything remotely like a bladed weapon in the passenger cabin: scissors, tweezers, nail files, etc.[14]

On a more general level, the events revealed a long list of security vulnerabilities in global transportation and border control systems (Koslowski, 2006, p. 89), especially with regard to the supervision/enforcement of visa and passport requirements. According to the findings, "at least two of the hijackers used altered passports, one…entered with a student visa but never showed up for class, three stayed in the US after their visa had expired, and several purchased fraudulent documents on the black market that primarily services illegal immigrants" (ibid.).

In pinpointing loopholes in pre-9/11 border control systems, the US government concluded that PNRs (both archived and real-time) were invaluable tools for investigating and thwarting terrorist attacks. Accordingly, the US Department of Homeland Security (DHS) was assigned, through its Bureau of Customs and Border Protection (CBP), the task of managing the collection, transfer and retention of PNRs.

America was shocked after the events of 9/11, but wanted to show that it was able to fight back, react quickly and provide a reliable defence that rendered impossible similar incidents in the future.[15] What America sought was nothing less than a "revolution in border security"[16] – analogous to the revolution in military affairs of the 1990s.

The "revolution" implied many individual measures from tightened border controls to a radical reorganisation of administrative structures; in view of our limited subject, we refrain from discussing too many details. What counts, however, is that 9/11 as well as the intended revolution had a direct impact on other countries, especially the allies in the near neighbourhood and in the transatlantic partnership.

On 19 November 2001, the US adopted a new Aviation and Transportation Security Act, which requires all airlines with US-bound international flights to submit a passenger manifest electronically. The Act stipulates that "the carriers shall make passenger name record information available to the Customs Service upon request".[17]

1.1.2.1 US–Canadian 'smart borders'

The US–Canada Smart Border Declaration signed on 3 December 2001 contains in sections 7–9 of the Action Plan thereto attached various airline-related security measures, in particular the sharing of advance passenger information (API) and PNR on high-risk passengers (s. 8) and the set-up of Joint Passenger Analysis Units (s. 9).

The internal Canadian requirement for airlines to provide API/PNR data had been adopted shortly beforehand, by the new Public Safety Act of 22 November 2001.[18] Although there had

---

[14] Refer to the Federal Aviation Administration rules adopted for US airports on 13 September 2001. Similar rules entered into force at Canadian and European airports. For the current EU situation, see the European Commission's list of 16.1.04 as amended on 5.10.06 to include explosive liquids; refer also to Regulation (EC) No. 2320/2002 of the European Parliament and Council, OJ L 355/1, 30.12.2002.

[15] The DHS was assigned/expected to "manage who and what enters our homeland" (Koslowski, 2006, footnote 6).

[16] See R. Falkenrath, Deputy Assistant to the President and Deputy Homeland Security Adviser, as cited by Koslowski (2006), p. 92.

[17] See the US code – Title 49, Subtitle VII, Part A, §44909, "Passenger manifests" (retrieved from http://www4.law.cornell.edu/uscode/49/44909.html).

[18] See Transport Canada (2001).

been no formal treaty commitment or request by the US, it is obvious from the overall scenario that Canada took this action as part of its post-9/11 solidarity and to be in compliance with the general standards set by the 'senior partner', according to a traditional pattern in US–Canadian relations. The same holds true for the Canada Anti-Terrorism Act adopted rapidly after 9/11 as a mirror image of the US Patriot Act.[19]

It should not be overlooked that Canada – although not itself a target of the September attacks – had already experienced its own encounter with airborne terrorism and its wider context. The Canadian sensitivity towards airborne risks relates to two tragic events, i.e. the bombing of Air India flight 182 in June 1985, which until the 9/11 events had been the single deadliest terrorist attack involving aircraft.[20] The attack that killed 329 persons en-route from Montreal to India was attributed to a group of Sikh separatists living in Canada.

The second incident is seen as one of the most consequential cases of data mismatch in counter-terrorist targeting: Maher Arar, a Canadian citizen of Syrian origin, spent almost a year in a Syrian prison cell due to false conclusions drawn from correct PNR data by the US and Canadian enforcement authorities. When it eventually became clear that there was no valid evidence against him, the Canadian government awarded Arar CAD 10.5 million (€6.9 million) in compensation, the highest settlement by the Canadian government in an individual human rights case.[21]

1.1.2.2 Transatlantic relations (EU–US and EU–Canada)

Post-9/11 solidarity also prevailed on the other side of the Atlantic: the EU heads of state and government met for an extraordinary European Council meeting on 21 September just 10 days after the events – a sign of truly exceptional consternation. In support of the transatlantic partners in distress, a number of important measures were put on track such as the European Arrest Warrant and the Framework Decisions on terrorism and on the freezing of assets of those suspected as terrorists.

Still, airline passenger data was not among the areas initially considered for cooperative action; much rather, the EU became concerned with it in an indirect manner. In accordance with their domestic legislation, since January 2003 US Customs[22] (and later the Canada Border Services Agency (CBSA)) has required Europe-based airlines to submit information on US-bound air passengers (Guild & Brouwer, 2006). While some of the companies immediately complied with the request – even allowing US Customs to collect the relevant data directly from the airline databases (CRS/GDS), others refused on the grounds that the transfer would violate EU data protection provisions. Essentially, "European airlines were presented with the choice of either breaking US laws, facing fines and potentially losing landing rights, or violating EU data protection laws and facing fines" (Koslowski, 2006, p. 97).

Reacting to this threat, the European Commission started negotiations with the CBP, which eventually led to the conclusion of the 2004 EU–US Agreement in PNR matters.[23] The 2004 Agreement itself rests on two vital pillars, i.e. the EU adequacy finding that the data will be

---

[19] Refer to the article "Canada's Anti-Terrorism Act", *Maclean's Magazine*, 25 October 2004 (retrieved from http://www.thecanadianencyclopedia.com/index.cfm?PgNm=TCE&Params=M1ARTM0012675).

[20] See the article "Air India Flight 182" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Air_India_Flight_182).

[21] For a detailed description of the case, see UK Parliament, House of Lords (2007), p. 12.

[22] This is based on the US Aviation and Transportation Security Act of 19 November 2001 and the Enhanced Border Security and Visa Entry Reform Act of 14 May 2002 (EPIC, 2007).

[23] See the EU–US Agreement of May 2004 (cited in appendix I of this report).

"adequately protected" in the US ('safe harbour' situation) and the related "Undertakings" by the CBP that such protection would effectively be granted.[24]

A corresponding API/PNR system was set up in Canada in 2002 under section 107.1 of the Customs Act (Bill C-17), with the collection of API data beginning on 7 October 2002 and that of PNR data on 8 July 2003.[25] Accustomed to the situation from previous experience with the US, the EU reacted swiftly and entered into negotiations that led to the EU–Canada Agreement in API/PNR matters of 3 October 2005.

As regards EU–US relations, however, the peace did not last long; following challenge by the European Parliament, on 30 May 2006 the European Court of Justice (ECJ) annulled the Agreement for lack of legal basis.[26] Negotiations then recommenced under time pressure in order to avoid a legal vacuum and the same Scylla/Charybdis scenario as had existed back in 2003. The new Agreement signed in July 2007,[27] with hardly any improvements in comparison with its predecessor, is far from pleasing all the parties involved. While European privacy commissioners point to a long list of deficiencies in the data protection arrangements, the US is about to launch a new series of bilateral agreements with some of the member states that might weaken privacy provisions to a still greater extent.[28]

With this situation in mind, the future seems uncertain as to whether it will entail more or less data protection. And there are yet further factors of uncertainty: so far just a passive player in PNR matters, the EU might reconsider its position and adopt a more proactive role by requesting air passenger data for all EU-bound flights. Be it for reasons of a new approach to border security (European Commission, 2008) or just a retaliation measure against the US, such a practice would by all means reshape the entire transatlantic landscape.

This background is all the more a good reason to consider EU–Canada relations with increased attention.

1.2 PNR & co: A methodology to turn commercial records into investigative tools

Airline data quite obviously exercises a strong attraction to crime and terrorism investigators as well as policy-makers, but one has yet to define where the attraction lies, whether this is a target worth going for and, finally yet importantly, how law enforcement access to and the exploitation of such data should best be implemented.

First of all, one should be aware that airlines are confronted with two types of data requests that should not be confused: **PNR** (passenger name record) and **API** (advance passenger information) are often mentioned in the same breath, which is in a way understandable as both

[24] For a detailed description of the PNR instruments, see sections 2.2 and 2.3 of this report.

[25] For details, refer to the Article 29 Working Party (2004), p. 5*ff*.

[26] See the Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union* [2006] ECR-I 4721 (cited in appendix I of this report); see also subsection 3.3.2 of this report.

[27] Refer to the EU–US Agreement of 23–26 July 2007 (cited in appendix I of this report); see also subsection 3.3.3 of this report.

[28] See the Czech Republic–US Agreement of 26 February 2008 (cited in appendix I of this report); see also subsection 3.3.4 of this report.

obligations concern passengers and have to be complied with before take-off. Furthermore, both subjects are occasionally regulated in the same legal instrument.[29]

API, however, has nothing to do with records established by airlines for their own commercial purposes. Although the imposed access to the PNR has frequently been characterised as a bold move by security agencies to jump on the bandwagon, API concerns data that airlines did not store previously but which they now have to collect separately for the benefit of border authorities. Roughly speaking, API includes all those data elements that travellers have to present at the border control in the destination country; API transmission resembles a pre-arrival manifest sent to the border authorities of the destination country.[30] In various respects, this represents considerable extra work and liability risks that airline associations view with some scepticism (ICAO, 2008).

1.2.1 Data collection through PNR and API

Collecting passenger data depends on the kind of mechanism concerned: the **API** data mechanism represents nothing but a "passenger surveillance and immigration law enforcement function carried out by the airlines on behalf of governments" (Hasbrouck, 2007). It consists, in the ideal case, of data that can be directly taken from the machine-readable part of a passport plus the general flight-related data that are anyway in the airline computers, e.g. as required under Directive 2004/82/EC (Council of the European Union, 2004).[31]

The list includes the following elements that are of evident interest to investigators as they enable the identity of a person to be directly established:

- number and type of travel document used
- nationality
- full names
- date of birth
- the border-crossing point of entry into the territory of the member state(s)
- code of transport
- departure and arrival time of the transportation
- total number of passengers carried on that transport
- the initial point of embarkation.

The current list means a relatively modest additional burden on the shoulders of airlines, but there are plans for extended lists that will be much more difficult to handle and are therefore vehemently opposed by the associations (ICAO, 2008).

---

[29] Refer to the Canadian Advance Passenger Information/Passenger Name Record (API/PNR) programme based on section 107.1 of the Customs Act, Passenger Information (Customs) Regulation, para. 148(1)(d) of the Immigration and Refugee Protection Act and Regulation 269 and of the Immigration and Refugee Protection Regulation.

[30] See the article on the Lufthansa website, "API (Advance Passenger Information)" (retrieved from http://www.lufthansa.com/online/portal/lh/cmn/generalinfo?l=en&nodeid=1795851&cid=).

[31] It should be noted that at least two EU member states, i.e. Spain and the UK (for targeted countries), have started to collect API from incoming passengers while PNR collection is not yet foreseen (Statewatch, 2007).

In comparison with API, the **PNR** system is a different "kettle of fish" (Statewatch, 2007); its added value for security purposes is not quite as obvious – which is due to the primarily commercial background for which it was created. The collection of PNR data has never been imposed by government authorities; air carriers have developed the system according to their own practical needs and those of travel agents and consumers in facilitating air travel and international bookings. This situation hampers the simple exploitation of PNR data in various ways:

- **Lack of uniformity** of PNR lists and airline databases

  To comply with International Civil Aviation Organisation (ICAO) standards, it is sufficient that the PNR contains the following five basic elements, just the minimum set of data necessary to complete a booking:[32] 1) name of the passenger(s), 2) contact details for the travel agent of the airline office, 3) ticketing details, 4) itinerary of at least one sector and 5) name of the person making the booking (ICAO, 2004, p. 2). All the remaining fields (up to 55) have been added according to the individual needs of airlines and their partners (ibid., p. 3).

  The lists used by different airline CRS/GDSs may contain the same data fields but the fields are presented under different names and in a different order. Sometimes fields are split into two, or vice versa several fields are regrouped under one heading, which seriously hampers the smooth comparison and evaluation of records collected by the airlines.

  How difficult data evaluation turns out to be in this unstructured environment is furthermore illustrated by the striking divergence of the lists of data that governments want to collect from the airline industry. None of the lists attached to the four EU instruments so far existing/proposed in PNR matters (the 2004 EU–US Agreement, the 2005 EU–Canada Agreement, the 2007 EU–US Agreement and the 2007 draft Framework Decision) are alike.

  In some cases, it is just a change of terminology, i.e. the same subject bears another label, whereas in others the order of subjects has been altered, which adds to the confusion in view of the length of the list (up to 34 items). Most of all there is the tendency to present shorter lists without sacrificing any content. This is particularly true for the 2007 EU–US Agreement, which in an (alleged) effort to comply with privacy-related criticism shortened the list of items from 34 to 19 – but only two data elements were effectively deleted while all the rest reappeared under another heading.[33]

- **Commercial orientation** of the data collected

  Many fields are of a more technical nature (e.g. seat number and ticket number) and do not reveal any security-related features, at least not at first sight. The spontaneous interest of investigators will probably turn to the so-called 'open fields' – SSRs, OSI and 'general remarks'. It is here that one would find references to special dietary preferences, health needs or similar elements that in turn could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or characteristics concerning the health or sex life of the passenger. On the other side, such sensitive data

[32] More precisely, this is in order to make the booking compliant with the IATA *Reservations Services Manual* (see ICAO, 2004).

[33] See the detailed comparison published by Statewatch (2007), p. 6.

whenever found in these fields should be seen as 'off limits' for security staff (see European Commission, 2004 with regard to the 2004 EU–US Agreement).

So all that the PNR can possibly deliver would require a painstaking screening of the technical data items in the hope of establishing patterns and matches with specific crime/terrorism-related data collections. This aspect will be deepened under section 1.2.3 below.

1.2.2 Data transfer from the airline industry to security authorities: 'Pull' vs. 'push'

Once again, we can see an important difference between the data systems originally designed for commercial purposes and those with an immediate surveillance background, such as API systems (APIS). While the primary enforcement/surveillance mechanisms seem all of a piece, the 'tapping' of commercial systems does not work quite as smoothly.

For **API** data the state of affairs is close to that of full automation: since the data currently required by the ICAO standard is limited to information contained in the machine-readable zone of EU passports,[34] it is sufficient that the passport be scanned ('swiped') at the airport check-in counter. The data is thus immediately available for use by the advance passenger processing (APP) system, which will run checks against security and intelligence watch lists connected to the system. Also known as the 'board/no-board' and 'red light/green light' system, the APP transmits the data to border control agencies prior to flight departure and receives in turn a directive for each passenger either permitting or denying boarding (ICAO, 2004a).[35] In the case of Canada, the API system is PAXIS (Passenger Information System), in which the data is transmitted to the Canadian authorities only *after* the departure of the flight (ICAO, 2003).

PNR processing proves to be more laborious and complex owing to a number of factors: as has been laid down in more detail above, airline PNR systems have not been conceived for security purposes in the first place, either in their technical architecture or in the content stored and processed. Furthermore, companies handling PNR data at the airline or distribution system (GDS) level have neither the skills nor the interest in performing the filtering of passenger data in favour of the security services. Especially in the early times of PNR exploitation for security purposes, it became almost a standard that air carriers left the filtering to the government authorities in charge, granting them direct access to their computers (the 'pull' method) rather than sorting out the relevant data themselves and transmitting it to the authorities (the 'push' method).[36]

In the past, US-based airlines simply gave their database passwords to US Customs, which allowed them to directly extract (pull) all the PNR data without previous filtering (Koslowski, 2006, p. 97). A still greater risk lies in providing access to the departure control system, as this system concerns data not confined to an individual flight but comprises the entire set of data held by the air carrier (EPIC, 2007).

---

[34] It should be noted, though, that Canada requires airlines to transmit with the API certain data elements that are stored in the reservation record (PNR) for the passenger concerned, especially the reservation record locator (ICAO, 2003). Airlines have apparently arranged to comply with this requirement (see the Lufthansa notice, retrieved from http://www.lufthansa.com/online/portal/lh/cmn/generalinfo?l=en&nodeid=1795851&cid=).

[35] The US CBP calls this process 'AQQ' (APIS Quick Query) leading to a "cleared" or "not cleared" message being sent back for each passenger (Statewatch, 2007).

[36] For details, see ICAO (2004), p. 4.

The 'pull' method has in the meantime been recognised as being in clear violation of privacy rights as laid down at the international level by the OECD guidelines of 1980.[37] It is also held to be in violation of corresponding legislation at the national level: without going into too many technical details at this stage, the direct access by third parties to an entire database for the purpose of obtaining just a limited set of data has to be considered a breach of the established principles of necessity and proportionality (EDPS, 2007).[38] It is not sufficient that the foreign security authority (in the case of EU–US relations, the US CBP) commit themselves to deleting the 'surplus' data at a later stage. Appropriate protection of passenger interests requires that such data be filtered before and not after its transmission to a third country.

If the push method has thus been identified as the only acceptable option in the transmission of passenger data (EDPS, 2007, para. 98), this does not exclude that its full implementation still faces considerable difficulties within the airline industry. There are frequent complaints that push systems are too expensive, whereas the pull method would involve relatively fewer additional expenses (ICAO, 2004, p. 4) (see Box 2)

Box 2. Who bears the costs?

It is stressed that the initial costs to support the pull method are relatively minor in comparison with the "significant initial up-front programming expense" arising from the development of a mechanism to positively extract data on affected flights and push the material to the requesting government agency. There is a consensus, though, that operating costs arise under both methods: for carriers operating a large number of flights in an affected market, these costs could run to "hundreds of thousands of dollars per year".

The air transport community feels that the transfer of PNR data – no matter by which method it is carried out – represents an intelligence gathering operation that lies solely in the interest of the state and not of the air carriers. Consequently, all costs associated with the operation should therefore be borne by the government(s) requesting the data.

Source: ICAO (2004).

Independent of what the cost situation is, one should be aware that only the push method appears in compliance with the privacy legislation and that those carriers continuing to use the pull procedure may be exposed to possible liability claims filed by passengers concerned. After years of discussion,[39] the EU finally accepted that member states, "together with users", may contribute to the costs of more stringent security measures to protect civil aviation against acts of unlawful interference. In order to avoid the risk of unlawful state aids, the new Regulation of 11 March 2008 also stresses that the subsidies "shall be directly related to the costs of providing the security services concerned and shall be designed to recover no more than the relevant costs involved" (European Commission, 2008a, Art. 5).

[37] See OECD (1980).

[38] In terms of the OECD 1980 guidelines, proportionality and necessity are considered sub-items of data quality (EDPS, 2005). For further details, see section 2.1 of this report.

[39] See the European Commission's (2006) report of 1 August, which concludes that the implementation of Community legislation on airport security is a task that is "typically that of a public authority" and that "the financing of transport security measures which form part of essential functions of the State and which are connected with the exercise of powers which are typically those of a public authority does not constitute State aid in the sense of Art. 87(1) EC Treaty" (European Commission, 2006, p. 5*f*.).

1.2.3 Exploitation of PNR data by security authorities

The exploitation of the passenger data obtained represents in a way the 'ultimate leg' for coming full circle: according to risk analysis-based security concepts (as they are nowadays a common standard), individual findings made during routine checks or through specialised enquiries are not to be seen as isolated events but also as elements that might make sense in combination with items found elsewhere, just like pieces of a big puzzle.

In the case of the PNR, the situation is particularly obvious: none of the data retained in such records would on its own reveal a specific threat or even suspicious indicators of threat. Contrary to the above-mentioned API data, which may produce a direct hit on a watch list and lead to a concrete fly/no-fly decision, the PNR has no such straightforward content.

The more 'discreet' significance of the PNR holds true for simple items (seat number, date of reservation, etc.) just as much as for the more sensitive SSR or OSI fields that potentially reveal passenger preferences and other circumstances such as "won't fly on the Jewish sabbath", "uses wheelchair" (Hasbrouck, 2007). The PNR is just a small cogwheel in the big machinery of global security – although one should always have in mind that even small wheels may produce big results, if they are placed in the right environment.

The only benefit one can expect from the PNR is therefore to produce results by running it against a series of data found in other border or law enforcement collections and see whether there are any matches. Such cross-checks are rather complicated when performed individually but their efficiency increases with the degree to which the system becomes automated.

This vision of exploiting PNR data thereby involves a twofold strategy, i.e. first, it is about scoring a hit on the passenger in question while running his/her data against watch lists and other data resources, and second, it entails widening the scope of information available when this data is retained and stored for future checks.

Major systems used for routinely scrutinising PNR data are discussed below.

1.2.3.1 United States

The US has certainly gathered the greatest amount of experience in the automated screening of airline passengers. Over the years, various names have surfaced such as the Computer-Assisted Passenger Prescreening System (CAPPS), CAPPS II, Automated Targeting System (ATS) and most recently Secure Flight. At the same time, confusion prevails over what is really going on. Even experts have to admit that they know just a minimum about the features and procedures involved – which appears hardly surprising in view of the secretive aura surrounding the fields of border surveillance and counter-terrorism. It is established that the US has tested and employed various programmes. We also know that some of them were abandoned (CAPPS I and II) owing to excessive error rates, but one can just puzzle over which system is currently operational: it is apparently not even certain whether "ATS is a predecessor or part of the Secure Flight program" (Rötzer, 2007).

CAPPS I and II

Like all its successors, the original CAPPS (first implemented in the late 1990s)[40] served to target potential terrorists by checking their PNR data against the Transportation Security

[40] It was implemented in response to terrorist threats perceived after incidents such as the explosion of TWA flight 800 and the Centennial Olympic Park bombing several days later in 1996 (see the article "Computer Assisted Passenger Prescreening System" in Wikipedia, retrieved from http://en.wikipedia.org/wiki/Computer_Assisted_Passenger_Prescreening_System).

Administration's (TSA) terrorism watch lists,[41] whereby passengers selected for special checks (so-called 'selectees')[42] became subject to additional luggage control to detect possible explosives. Other person-related checks were not foreseen. CAPPS fell into disgrace after 9/11 when it became known that several of the suicide hijackers had actually been selected by the system but that the controls had not been carried out.[43]

CAPPS II, launched in 2003 with the express backing of the US Patriot Act, extended checks to all passengers, irrespective of whether they had checked in luggage. It was run by a government agency (the TSA), instead of the commercial carriers as had been the case under CAPPS I. There was an expanded selection of PNR data that had to be run against government records and furthermore private-sector databases. The result in terms of a 'risk score' was displayed on the boarding cards, whereby green meant 'no threat' (no additional screening), yellow 'unknown or possible threat' (additional screening) and red 'high risk' (no fly). CAPPS II was cancelled in the summer of 2004, mainly on the basis of a devastating report by the US General Accounting Office stating that CAPPS II had not done its homework in seven out of eight areas for which improvements had previously been requested (US GAO, 2004). Specific criticism was directed against the high error rate affecting the watch list with prominent victims such as Senator Edward Kennedy (EPIC, 2007a), the absolute lack of transparency as to how the list was established and finally the employment of doubtful private information resources. The passengers concerned had neither access to the data nor ways to challenge an unfavourable risk designation (Greenemeier, 2004).

Automated Targeting System

While the public still speculated about the creation of a CAPPS III system, the DHS CBP had already extended its ATS, originally conceived to "target ocean-going cargo containers for inspection", to include travellers. Its new function was discovered only in November 2006, when the DHS published a "Notice of Privacy Act system of records"[44] requesting exemption from crucial provisions of the Privacy Act of 1974 (EPIC, 2007c). Again, criticism was overwhelming: not only were the ATS terrorist risk profiles to be "secret, unreviewable and maintained by the government for 40 years", there were also technical deficiencies haunting the ATS even in the performance of its limited container-related tasks. These deficiencies resulted in low marks ("C-/D+") in a 2006 scrutiny report by the House Homeland Security committee and made it appear entirely unqualified to handle a still greater amount of data (ibid.). Given that its techniques were considered "imprecise", it was felt irresponsible to allow the ATS to "mine a vast amount of data to create a 'risk assessment' on hundreds of millions of people per year, a label that will follow them for the rest of their lives, as the data will be retained for 40 years" (EPIC, 2007c).

Despite considerable system changes announced by the DHS in August 2007 (the cancellation of exemptions from the Privacy Act and establishment of comprehensive passenger redress

---

[41] See Privacy International (2007).

[42] This relates to those found on the 'selectee' list administered by the TSA as opposed to the 'no-fly' one equally managed by the TSA (refer to Privacy International, 2007).

[43] See the article "Computer Assisted Passenger Prescreening System" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Computer_Assisted_Passenger_Prescreening_System).

[44] See US DHS, Office of the Secretary, Privacy Act of 1974: System of Records, *Federal Register*, 71, no. 212 (November 2, 2006) (retrieved from http://edocket.access.gpo.gov/2006/06-9026.htm).

procedures under the DHS TRIP programme),[45] the current operation of the ATS and its relationship to its Secure Flight counterpart largely remain in the dark.

Secure Flight

Almost simultaneously with the ATS announcement, the DHS presented its new Secure Flight programme[46] to conduct uniform prescreening of passenger information against federal government watch lists for domestic and international flights. In its screening routine, the Secure Flight programme intends to identify "suspicious indicators associated with travel behaviour" in passengers' itinerary PNR data (EPIC, 2007a). Because of the numerous security vulnerabilities detected by government reports as early as 2006 (Privacy International, 2007) including "significant weaknesses" in the terrorist watch lists available,[47] it seems that the official operation of the Secure Flight programme will remain grounded until 2010. Public trust in the watch lists has also been undermined by news reports according to which air marshals were subject to a "quota system in reporting terrorist profiles".[48]

Still, one cannot be sure what is really going on; reports are contradictory and it seems that under the auspices of secrecy, government sources avoid providing a comprehensive description of all the activities underway in air passenger screening. Characteristically enough, none of the reports dealing with the ATS wastes a word on Secure Flight and vice versa.

1.2.3.2 Canada

In Canada things appear less complicated, as one might easily tell from consulting the website of the CBSA: there is just one agency in charge (CBSA), one programme to check PNR and API (PAXIS) and a concise and understandable description accessible to all those interested in the matter.

PAXIS

The PAXIS system, created in 2002 in the follow-up to the Canadian Anti-Terrorism Act of 18 December 2001,[49] provides an automated risk assessment of pre-arrival data transmitted by air carriers to the CBSA through electronic data interchange, e-mail and the Internet (TBCS, 2005).

In contrast to corresponding US systems, PAXIS deals with the API and PNR in absolutely the same manner: the API data does not even need to be transmitted before the plane departs; it is sufficient if the transfer takes place within 15 minutes before landing in Canada. This implies that Canada – at least so far – does not employ the no-fly option, i.e. to interdict, in the case of high-risk travellers, the boarding of the aircraft at the airport of origin. All that PAXIS does in

---

[45] See US DHS, Office of the Secretary, Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System, *Federal Register*, 72, no. 150 (August 6, 2007) (retrieved from http://edocket.access.gpo.gov/2007/E7-15198.htm).

[46] See the US DHS Press Release of 9 August (US DHS, 2007a).

[47] See "Terrorism Watch list is Faulted for Errors" (Nakashima, 2007, p. A12) (retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601386.html).

[48] For promotion purposes, "[e]ach federal air marshal is now expected to generate at least one SDR [surveillance detection report on air passengers] per month". See the *Denver News* article, "Marshals: Innocent People Placed on 'Watch List' to Meet Quota", 21 July 2006 (retrieved from http://www.thedenverchannel.com/news/9559707/detail.html).

[49] See Parliament of Canada, Bill C-36, Anti-Terrorism Act (2001) (retrieved from http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Parl=37&Ses=1&Mode=1&Pub=Bill&Doc=C-36_4).

this context is a pre-arrival targeting of travellers in the sense that it recommends certain persons be intercepted for secondary inspection upon arrival (CBSA, 2008a).

Technically speaking, PAXIS – on the basis of previous API/PNR data contained in the system – flags risk passengers with at least one risk element in their record, i.e. those "who reach at least one national security threat threshold" (ibid.). It is to be noted that PAXIS assigns a risk score to flagged passengers, but it is the national/regional risk-assessment officers who take the ultimate decision whether and how to conduct the secondary inspection. This certainly helps to avoid embarrassing errors that seem so significant with fully automated lists, as for instance in the US.

Similar to the EU–Canada Agreement, the PAXIS risk assessment and targeting system has evoked very little concern, among the passengers, privacy authorities or non-governmental organisations (NGOs). The most important factors for this positive appreciation may be the following:

- the absence of fully automated mechanisms such as no-fly orders in combination with unreliable watch lists;
- a common sense adjustment of the automated PAXIS risk score by the targeting specialists of the National Risk Assessment Centre (CBSA);
- full transparency of the screening/targeting procedures employed;
- access to redress procedures for the passengers affected;[50] and
- continuous improvement of the PAXIS system rather than frequent system change.

The satisfaction rate among users and officials concerned has been exceptionally high: unlike in the US, there has been no outcry for reform by either passengers or government commissions, which would provoke a need for radical reforms.[51]

That being said, one also needs to look at another, more recent aspect of Canadian threat-prevention that clearly attracts much less applause.

Passenger Protect Programme (Passenger Information System of the Customs and Border Service)[52]

Since 18 June 2007, Canada has operated the Passenger Protect Programme with a no-fly mechanism as its centrepiece, very much in line with the abovementioned US examples. The new rules, adopted as government regulations (with no involvement of parliament!) under the Aeronautics Act[53] and the authority of the minister of transport, foresee the establishment of a no-fly list, comprising individuals who are

a) involved or suspected of being involved in a terrorist group and who can be reasonably suspected to endanger the security of any aircraft,

b) convicted of one or more serious and life-threatening crimes against aviation security, or

---

[50] Refer to the CBSA's Interim Memorandum D1-16-2 (CBSA, 2003).

[51] Instead, a recent evaluation study has shown that there is a high rate of approval of the 6-year old system among targetters at the national and regional risk assessment centres (62% and 83% approval, respectively) (CBSA, 2008a, p. 16*f*.).

[52] For a programme description, see Transport Canada (2007a).

[53] This is based on sections 4.76, 4.77 and 4.81 of the Canadian Aeronautics Act of 1985 (retrieved from http://laws.justice.gc.ca/en/ShowFullDoc/cs/a-2///en).

c) convicted of one or more serious and life-threatening offences and who may attack or harm an air carrier, passengers or crew members.

The list compiled by Transport Canada (with some involvement of justice, enforcement and intelligence services) is implemented by the airline companies, which have to report back each time a traveller "matches at check-in in name, date of birth and gender with someone on the list" (Transport Canada, 2007a). Transport Canada's 24-hour service will in turn take an immediate decision on whether to issue an "emergency direction that the individual poses an immediate threat to aviation security and should not be permitted to board the flight".

As an exceptional measure of protest, the privacy commissioners of Canada adopted a joint resolution claiming that the new mechanism violated legal provisions and good reason in various respects (OPC, 2007a), through the

- lack of a legal basis in the Aeronautics Act for adopting such a programme;
- lack of adequate protection, under the current Privacy Act, against the privacy risks resulting from such an initiative;
- absence of an available safeguard against the sharing of the list with other countries;
- further violations of privacy rules such as collection/use/disclosure of sensitive and excessive personal information; secretive use of that information; lack of a legally enforceable right of appeal for the traveller; and
- indications that Transport Canada will use not only the Canadian no-fly list but also corresponding lists established by other countries.

Canadian privacy commissioners consider it very disappointing that the government has not taken up any of the critical remarks or suggestions contained in the resolution: "The government did not respond except to express its commitment to the Program."[54] It is stressed, however, that this is "a Transport Canada not a CBSA program", so one should not draw any premature conclusion about a general change of attitude in border matters. On the other hand, it may also be a worrying aspect that services outside the traditional security sector engage in stringent law enforcement activities without being familiar with the rules and ethics of this field.

From a European point of view, the extent to which international flights are/will be affected by the programme is not apparent: at least flights from and to EU destinations seem to be exempt. As laid down above, the EU–Canada Agreement in API/PNR matters is very clear about the API/PNR data – they do not have to be transmitted before departure and will be used for a secondary screening only, which logically excludes any no-fly option.

1.2.4 Results expected and those obtained

Despite the full trust and high expectations that policy-makers exhibit when introducing stringent measures in transport and border security, hard evidence on the positive impact of such initiatives is quite scarce.

In many cases, this is rooted in the secrecy surrounding this sensitive field, which impedes the detailed description of individual cases. Such problems are encountered even by official evaluation mechanisms, e.g. the joint review undertaken in September 2005 under section 5 of the 2004 EU–US Agreement on PNR matters. The European Commission report on this event complained about the "limitations imposed on the number of records that could be accessed and

[54] Derived from a letter by C. Baggaley, Strategic Privacy Adviser at the OPC to the author of 5 May 2008. He stressed, however, that "very few, if any, passengers have been denied boarding".

on the provision of hard copy versions of certain staff procedural guidance" (European Commission, 2005, p. 6).[55] Equally, Canada's Privacy Commissioner Jennifer Stoddard was disappointed to hear that the new watch list/no-fly programme was based on "practical global experience and risk assessment rather than specific studies".

It can be hoped that the forthcoming review of the EU–Canada PNR Agreement will shed some additional light on the working of the passenger data mechanism.

1.2.5 Financial considerations: Costs/liabilities involved for airlines, states and passengers

There is perfect agreement that security, together with infrastructure, open skies and the environment represent the biggest challenges for airlines.[56] According to the International Air Transport Association (IATA), since the 9/11 attacks the airline industry has incurred an "additional $5.6 billion annually in new security costs". And airport security fees are constantly rising as is shown for both European and Canadian airports.[57]

It seems accepted in general that security costs should be shared among the various parties concerned, i.e. they "should be borne by the State, the airport entities, air carriers, other responsible agencies, or users" (Art. 5 Regulation (EC) No. 300/2008),[58] whereby there is disagreement as to the respective size of these shares. The EU exceptionally allows state aid insofar as it is directly linked to security purposes (ibid.).

As regards the airlines, the PNR costs no longer seems a subject of primary dissatisfaction; after initial ICAO estimates amounting to "hundreds of thousands of dollars per year" just for running an existing push or pull system (ICAO, 2004, p. 4), this topic no longer shows up in recent publications – possibly owing to established cost-cutting routines. The European Commission currently estimates PNR costs at €0.20 per passenger.[59]

Another way to determine the financial impact is to look at the travel industry, whose profits went down by 30% following the introduction of tougher security measures: according to them European travellers tend to turn to destinations with less cumbersome entry conditions (Koslowski, 2005).

---

[55] Refer also to the European Parliament Resolution P6_TA-PROV(2007)0347 of 12 July 2007 on the PNR Agreement with the United States of America (retrieved from http://www.statewatch.org/news/2007/jul/ep-pnr-resolution-jul-07.pdf).

[56] See the article by D. Grossman (2007) on comments by IATA Director General Giovanni Bisignani.

[57] In Canada, for domestic itineraries the air travellers security charge (ATSC) is currently CAD 5 one-way up to a maximum charge of CAD 10. For trans-border itineraries, the ATSC is CAD 8/USD 7 one-way up to a maximum charge of CAD 16/USD 14 – see the Air Canada online article "What are the additional charges in my fare?" (retrieved from http://www.aircanada.com/shared/en/common/flights/pop_surcharge.html).

Regular complaints are also heard in Europe, e.g. in the UK that "Heathrow's charges should rise from £9.28 to £10.96 per passenger while Gatwick's charges should rise from £4.91 to £5.48" – see the *BBC News* online article "Watchdog eyes raised airport fees", 3 October 2007 (retrieved from http://news.bbc.co.uk/2/hi/uk_news/7025419.stm).

[58] Refer to European Commission (2008a).

[59] This information was provided by the European Commission (DG for Justice, Freedom and Security) on 10 April 2008.

2. PNR and the wider security landscape

As shown in the previous section, the PNR on its own cannot achieve a significant enhancement of airline or border security. Even within the (small) sector of screening and targeting passengers, the PNR needs to be embedded in a network of links to other data and human resources.

2.1 Visions of a perfect border: Seamless protection and extra-territorial action

This interdependence is all the more crucial when looking at security from a larger perspective: 'total security' as is increasingly strived for on both sides of the Atlantic requires an interlocking of all tools employed in the wider context of travel and migration control.

2.1.1 Tendencies in travel and immigration control

The Western world finds itself ever more challenged by complying with the contradictory targets of a maximum of mobility on the one hand and a maximum of security on the other.

Since border-related security in its traditional meaning – i.e. controls based on thorough and time-consuming physical checks – can clearly not achieve this goal, information technology and automation are often seen as the way out. As a sort of miracle solution, the IT approach promises to transform borders into insurmountable obstacles for any illegal traveller/migrant while hardly impeding the bona fide passenger. Besides conferring a maximum amount of checks into the domain of IT, biometrics and automation, the key to overall control of the territory lies in the achievement of a faultless entry–exit system.

It is also part of the streamlining approach to prevent the system from being overburdened by too many 'difficult' cases awaiting clearance right on the border, mostly within the territory of the receiving state. This explains the tendency to 'push out borders' to extra-territorial locations.

Nevertheless, one should not conceal the fact that the 'perfect border' as envisaged is costly in various respects, i.e. financial and human resources as well as sacrifices in terms of civil liberties. And beyond all this, there are considerable doubts about the extent to which the changes envisaged really deliver the results promised. US experience indicates that a border perfectly sealed-off at its airport entries is rather worthless as long as the 'back doors' along endless land and water borders remain wide open. So far, no one seems to possess the technical means to resolve the core problem of reconciling the surveillance and mobility objectives in the case of a voluminous, cross-border commuter community.[60]

The following remarks intend to outline major solutions proposed under the auspices of both 'tight and streamlined borders' and 'extra-territorial controls' in order to obtain a clearer picture of the neighbourhood in which PNR will henceforth do its job.

2.1.1.1 Tight but streamlined borders

The **US** set the pace back in the 1990s when it introduced **US-VISIT**, the first "automated entry–exit system" originally conceived for immigration purposes to detect visa over-stayers (US DHS, 2007). The system secures the identity of the visitor by means of biometric identifiers, i.e. two index fingers digitally scanned and a digital photo taken at the US port of entry, which are entered into the Automated Biometric Identification System (IDENT). At exit, the identity of the

[60] For further details, see section 4.3 of this report.

traveller is again checked by means of comparison with the data stored in IDENT.[61] The US-VISIT/IDENT system provides, by the way, for a far-reaching interoperability with the databases managed under the aegis of the DHS. Biometric exit controls are facilitated by automated, self-service kiosks that are integrated with the airline check-in procedures.

The system is air-tight insofar as it includes – in principle – all travellers, no matter whether they are subject to visa obligations: the former privilege of the so-called 'visa-waiver' countries[62] was abandoned in 2004.[63] The only remaining exemptions from the US-VISIT system are valid for Canadian citizens in general and certain groups of Mexicans.

The US does not currently employ a 'bona fide traveller' programme to expedite entry–exit control for foreigners; it is only at US consulates abroad that 'bona fide' applicants may find simplified procedures when applying for a visa (US DHS, 2006).

Within the **EU**, up to now the coverage of entry–exit movements has been fragmentary: the **Schengen Information System** (SIS), the oldest border-related database system, contains data on certain groups of persons to be stopped at the border (e.g. persons requested for extradition, suspected of crime or unwanted in the territory of a member state). In its new **SIS II** generation, the system will allow identity checks on the basis of biometric information (facial photograph and fingerprints).[64] The **Visa Information System** (VIS) will hold biometric data (facial photograph and 10-digit fingerprints) to identify persons who have lodged a visa application with an EU member state (EurActiv, 2007a). And finally, **EURODAC**, a fingerprint database for identifying asylum seekers and irregular border-crossers, enables authorities to determine whether asylum seekers have already applied for asylum in another EU member state or have illegally transited through another EU member state.[65] Although the SIS II and VIS share a common technical platform, there is so far no interoperability between them or with EURODAC (Hobbing, 2007).[66]

In early 2008, the European Commission decided to reconsider the situation and presented its vision of a future European **entry–exit system** (European Commission, 2008a). On the theme of "the next steps", it proposes to introduce a fully fledged entry–exit system based on

a) the **registration**, in an entry–exit database, of all non-EU nationals entering EU territory.[67] The database would include data on the time/place of entry, the length of stay authorised

---

[61] For details, see Hobbing (2007).

[62] This includes the following EU member states: Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Luxembourg, the Netherlands, Portugal, Spain, Slovenia, Sweden and the UK. The only privilege that remains for VWP countries is that their citizens do not have to undergo the costly and time-consuming visa application procedures at a US consulate back home.

[63] After the attempt by a UK citizen (Richard Reid) to detonate a bomb hidden in his shoe in a transatlantic flight, consideration was given to abandoning the VWP altogether. Instead, the US Congress decided to keep the VWP but subject its beneficiaries to the requirements of the US-VISIT programme (see Koslowski, 2005).

[64] Refer to European Commission (2005a).

[65] Based on the biometric data stored, it is the first automated fingerprint identification system in Europe and has been operating since 15 January 2003; refer to the European Commission's website article "'EURODAC' system", last updated 10 January 2008 (retrieved from http://europa.eu/scadplus/leg/en/lvb/l33081.htm).

[66] This decision was taken in 2007 when the European Parliament, for reasons of privacy protection, insisted on keeping the systems apart (Ludford, 2007).

[67] The requirement would at first concern foreigners admitted for a **short stay of up to 3 months** (regardless of whether they require a visa!), by far the largest group entering the EU. Exceptions would be

as well as biometric data of the persons registered. In the case of 'over-stayers', the system would transmit automated alerts to the competent authorities;

b) the granting of a **registered traveller status** to low-risk travellers from non-EU countries who, after appropriate prescreening, could benefit from a simplified and automated border check; and

c) an **automated border-control system** to manage the entry–exit of both non-EU nationals (as far as they have the status of a registered traveller) and EU citizens.

The reception of these ideas has been mixed, with critics notably pointing to certain discrepancies between the dubious alleged benefits of the monumental border-control system proposed and the inconveniences in terms of fundamental privacy risks associated with such large-scale data collection (Geyer, 2008). Most of all, it appears doubtful whether the system really fulfils a facilitation need, given that neither EU citizens nor non-EU nationals in possession of a visa face any specific difficulties at the border.[68]

2.1.1.2 Forward defence and advance checks: Controls on foreign territory

From security-related history, we know that there have always been forward-oriented tactics in the sense of outpost strategies to keep possible trespassers as far away from one's doorstep as possible. Sometimes these strategies involved look-out posts or listening watches to capture the first signs of security threats approaching. When modern border management applies forward tactics, it is not satisfied with just a passive monitoring of trends,[69] but wants to do a proactive job by possibly intercepting 'undesirable elements' before they actually reach the border. The relocation of controls may also be motivated by concepts of risk prevention, e.g. to prevent persons with a possible terrorist profile from boarding a plane.

In addition, there is of course the effort to ease pressures on domestic ports of entry by anticipating formalities in the context of regular international travel. In order to facilitate arrival in the country of destination and avoid long waiting queues, there are mounting efforts to relocate formalities away from the border to foreign territory, often right into the country of origin of the traveller.

The most common extra-territorial formality is the **visa application**, which must be complied with in the country of origin, residence or temporary stay of the applicant. The requirements are broadly similar for visitors (subject to visa requirements) to Canada,[70] the EU[71] or the US.[72]

---

granted to holders of local border permits, national long-stay visa or residence permits as well as all those exempted from stamping (pilots, seamen of cruise ships, diplomats, etc.).

[68] For a very detailed discussion of the proposal and its apparent weaknesses, see Guild, Carrera & Geyer (2008).

[69] This may still have been true for the old-style drugs liaison officers stationed in the 1980s at major European airports. They had to observe tendencies, consult with colleagues from the host state and possibly assist them in interviewing travellers.

[70] See the Citizenship and Immigration Canada website article, "Visiting Canada: How to apply", last updated 14 June 2007 (retrieved from http://www.cic.gc.ca/english/visit/apply-how.asp#step5).

[71] See the German Federal Foreign Office website article, "Visas for entry into Germany", last updated 14 May 2008 (retrieved from http://www.auswaertiges-amt.de/diplo/en/WillkommeninD/EinreiseUnd Aufenthalt/Visabestimmungen.html.#t6).

[72] See the US Department of State website article, "How to get a Visa" (retrieved from http://www.unitedstatesvisas.gov/obtainingvisa/index.html).

Applications have to be submitted to their respective embassies/consulates[73] abroad. In most cases, a personal visit to the visa-issuing office is mandatory – only Canada leaves some discretion to the visa officer.

At the same time, visa procedures take advantage of extending certain e-border formalities to the 'outpost' location: during the interview, **US consulates** take digital fingerprints of the applicant, which together with all the other data will be run against watch lists (CLASS, NCIC, IBIS, etc.) containing criminal justice and other sensitive information. An IBIS/IDENT record for the US entry–exit system will then be created, which will virtually accompany the applicant during his/her entire travel to the US.[74]

The **EU** has been inspired by the US example: so far and according to Art. 48 of the VIS Regulation, the biometric data required for the **VIS** (i.e. a digital photo and 10-digit fingerprint)[75] is to be collected by the member states' consulates abroad[76] and subsequently entered by them into the VIS database. The information will thus be available in the system for identification purposes, once the visa holder arrives at the external EU border (European Commission, 2008b). The situation would be different, however, under a possible future entry–exit system for non-EU nationals not subject to a visa requirement: for them the necessary registration of biometric data would take place at the border on the occasion of their first entry into EU territory (European Commission, 2008a).

A clear signal in terms of keeping unapproved foreigners at a distance is also found in the **electronic travel authorisation (ETA)** concept, already practised for years in Australia.[77] Praised by its inventors for allowing "easy access to data on all travellers to Australia…[and supporting] maintenance of Australian border integrity by law enforcement and health authorities" (Australian Government, 2008), its introduction is now being considered on both sides of the Atlantic, as the "Electronic Travel Authorization" programme in the US[78] and as the "Electronic System of Travel Authorisation" in the EU.[79] The interesting and, at the same time, controversial element of ETA is that even citizens of (so far) visa-free countries could be subjected to some kind of advance control.

The US in fact foresees the new mechanism just for those countries still enjoying visa-free travel under the VWP (US DHS, 2006a) and the EU seems attracted to the same aspect

---

[73] A Schengen short-stay visa is granted to a non-EU national that allows him/her to travel in the entire Schengen area, and not just to the member state that issued the visa. See the EU/German instructions on the Schengen area in the German Federal Foreign Office website article, "The Schengen Agreement and the Convention Implementing the Schengen Agreement", last updated 17 December 2007 (retrieved from http://www.auswaertiges-amt.de/diplo/en/WillkommeninD/EinreiseUndAufenthalt/Schengen.html).

[74] For details, see Hobbing (2007), p. 10*f.*

[75] See Arts. 9(5) and 9(6) of the VIS Regulation as presented in the European Parliament's report (A6-0194/2007) on the Draft European Parliament Legislative Resolution (retrieved from http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2007-0194&language=EN&mode=XML).

[76] The gradual establishment of biometric collection facilities at the consulates will occur according to the roll-out plan laid down in Art. 48 of the VIS Regulation.

[77] The ETA was introduced in 1996. Unlike ordinary visas, when an ETA is issued, no stamp or other documentation is added to the holder's passport; instead, the computer-based system links the passport number to the ETA and is accessible by immigration officials (Australian Government, 2008).

[78] See the US DHS (2006a).

[79] See European Commission (2008a), p. 9.

(European Commission, 2008a). Held by the DHS as a "continuation of the VWP, it could just as readily (although less photogenically) be described as online visas for all" (Lettice, 2008).

Cheaper[80] and less cumbersome[81] than a traditional visa, it of course involves formalities unfamiliar to travellers who have been used to spontaneous travel decisions: "Why should tourists from visa-free countries announce their intentions 48 or 72 hours in advance?" (Joffe, 2007).

The outpost strategy also surfaces in the context of some less elegant aspects of EU border management. When migratory pressure increased on the southern front of the EU and the first African boat people arrived in Malta and the Canary Islands,[82] politicians from various countries excelled in ideas on how to stop the "human tragedies in the Mediterranean" combined with the trafficking of human beings (IRRI, 2004). First the UK (in 2003) and then Germany and Italy (in 2004) brought up the concept of offshore solutions in terms of so-called "offshore humanitarian processing centres" (Helmut, 2005) that would allow examination of asylum requests in a safe-harbour situation. Various sites were considered (Morocco, Romania and Ukraine), but the most concrete arrangement was achieved with Libya, which offered a camp near Tripoli for implementing the EU concept (ibid.).

Overseas processing centres are not new in global refugee policy; in the 1990s, the US was using its facility at the Guantanamo base(!) in Cuba to process Haitians trying to make their way to the US by boat. The Australians employed a similar idea in the wake of the Tampa crisis in 2001, creating processing centres for intercepted asylum seekers on the Pacific island nations of Nauru and Vanuatu (IRRI, 2004).

Although the first deportations from Italy had already started and the EU ministers of interior had, in principle, approved the creation of the centres, the project was abandoned towards the end of 2004. Besides vehement protest by human rights organisations all over Europe, the withdrawal was also motivated by the finding that Libya was not even a party to the Geneva Refugee Convention.

Yet another variation of extra-territorial intervention exists in the **posting of immigration control officers abroad** in order to prevent travellers with false/insufficient documents from boarding the aircraft. This is a uniquely **Canadian approach**, which has been successfully adopted by others, to stop terrorists, criminals and other undesirables. In recent years, Canadian officers abroad have stopped more than 33,000 persons with false documents before they boarded planes for North America (FAITC, 2003).

2.1.2 Further extra-territorial presence of control and law enforcement

Offshore solutions are a tempting alternative to purely domestic intervention against undesirable impacts from abroad. In some cases, conflicts of this kind may be resolved by cooperative efforts together with other partners based on mutual legal or administrative assistance, but mostly states prefer to do the job on their own if they can, relying on their expertise and skills.

---

[80] A service fee of AUD 20 (approximately €12.15) will be incurred for online lodgement (Australian Government, 2008).

[81] ETA applications will normally be lodged over the Internet (ibid.).

[82] See Kroeger (2007).

The most prominent example is the post-9/11 **Container Security Initiative (CSI)** launched in early 2002 with close cooperation between the US and the EU. Based on the insight that terrorist threats are not confined to human action but may equally involve the use of highly dangerous machinery/substances, as in the case of weapons of mass destruction (WMDs), the CSI aims at assisting the control of containers – which carry approximately 90% of international trade – outside US territory (Koslowski, 2006).

The reasoning behind this strategy is that the detection of WMDs after arrival in a US port may be "too late if the device can be detonated by remote control or the container is booby-trapped to detonate when opened for inspection" (ibid.). A second element is the usual congestion of major ports, which impedes the inspection of a significant share of containers.[83] The costs involved in the purchase and operation of refined technology are immense as well as the funds necessary for running the human interface, but they are "many times outweighed by the cost to the US economy resulting from port closures due to the discovery or detonation of a weapon of mass destruction or effect" (McClure, 2007).

The CSI agreement of 2004 (Council of the European Union, 2004a) is working smoothly to the satisfaction of both parties. It should be noted that the engagements are reciprocal: inspectors from EU member states could also be deployed to US ports, but member states have so far not yet made use of this option (Koslowski, 2006).

A more controversial item is that of **sky marshals** accompanying international flights – although a closer look at existing legal provisions shows that positions are not as far apart as one might believe from the EU–US clash on the air security memorandum of understanding (MoU) currently proposed by the US to the 27 member states (Traynor, 2008). In fact, the new Regulation on Civil Aviation Security (European Parliament, 2008) expressly allows member states to authorise the deployment of "in-flight security officers" (sky marshals), provided that they are government officials. It seems that rather than the substance it is the context of the US proposal with its link to "unacceptable new PNR demands" and the pressure exercised on individual governments (blackmail) that throws a negative light on the whole initiative.[84]

One last instance of public authority exercised abroad is that of '**extraordinary renditions**', i.e. the apprehension and extrajudicial transfer of a person from one state to another.[85] Widely outlawed, this practice was adopted by US intelligence services in the 1990s in order to counter terrorist threats more efficiently. As opposed to legal rendition, it refers to a form of rendition in which suspects are taken into US custody but delivered to a third-party state, often without ever being on American soil and without involving the rendering country's judiciary (Geyer, 2007). This practice and those who have probably taken advantage of it on European soil have been profoundly condemned by European institutions, in particular the European Parliament.[86]

---

[83] Before 9/11, the inspection of 2% of containers was the normal share in major ports. Since then, this ratio has improved although no exact figures are given; however, the ratio of prescreening has risen to 100% and there are now refined methods of risk assessment (refer to McClure, 2007).

[84] For further details on the proposal, see section 2.3.1 in this report on the new generation of commitments.

[85] Refer to Geyer (2007), p. 2.

[86] See the online article, "EU countries ignored CIA terror suspect flights, report says", *Guardian*, 14 February 2007 (retrieved from http://www.guardian.co.uk/world/2007/feb/14/eu.usa).

2.2 Legislative hotspots: Some crucial aspects in designing PNR mechanisms

Clearly, the drafting of legislation on the PNR and the sensitive areas connected to it involves quite a number of hotspots, i.e. legal and ethical issues whose handling would require in-depth examination.[87] In most cases, this occurs within the regular discussion on legal and practical features of existing and planned instruments.

There are, however, two items with more remote significance but which are still important for shaping PNR legislation in different regions of the world.

2.2.1 Transatlantic divide in security/privacy matters: (Continental-) European sensitivity towards border-related privacy intrusions vs. (Anglo-Saxon) North American sensitivity towards internal intrusions (ID card issue)

The recent clashes over complex issues such as Iraq (war or not), the right way to tackle terrorism (war or fight)[88] created or reaffirmed some of the well-known stereotypes of people on this and on the other side of the Atlantic.

Current attitudes wrapped in catchy formulas such as 'sensitive day-dreamers vs. tough cowboys' tend to be seen as immutable facts of life, arising out of the respective national characters.[89]

This same scenario under the adage "Americans are from Mars and Europeans are from Venus"[90] is likely to arise anew in our current privacy subject: 'old Europe' with its strong sensitivity towards privacy intrusions by means of collecting, processing and transmitting passenger data[91] forms a contrast to 'down to earth America', proud of not showing too many scruples when it comes to the "critical area of law enforcement and public safety".[92] The formula is catchy but it is also one-sided – given that the situation is just the other way round in a related area.

---

[87] Typical items are e.g. 1) choice of the body in control over data selection/transfer (push vs. pull systems), 2) the question of who is granted access to the data, and 3) the duration of data retention.

[88] The US side emphasises the military aspects of counter-terrorism ('war') whereas Europeans tend to consider this a police-related activity.

[89] See Pipes (2002), who at the same time recalls that "differences are hardly permanent. Two centuries ago, when Americans acted cautiously around the tough-guy Europeans, the roles were roughly reversed."

[90] This adage is taken from Robert Kagan's book, *Of Paradise and Power: America and Europe in the New World Order*, New York: Knopf, 2003.

[91] See the newest statistics, according to which 82% of European Internet users have little trust in personal data management over the web (Eurobarometer poll of 17 April 2008, as cited by EurActiv, 2008). As of 15 May 2008, the European Data Protection Supervisor Peter Hustinx has warned the Google corporation that the expansion of its 360, full-colour Street View map service to Europe might lead to expensive lawsuits for privacy violation (*EU Observer*, 16 May 2008, retrieved from http://euobserver.com/9/26154/?rk=1).

[92] On the EU draft Framework Decision on data protection in police and criminal matters, Paul Rosenzweig, Deputy Assistant Secretary at the DHS, states, "The draft seeks to apply the same tired, failed standards of adequacy that it has applied in its commercial laws. …The EU should reconsider its decision to apply notions of adequacy to the critical area of law enforcement and public safety. Otherwise the EU runs the very real risk of turning itself into a self-imposed island, isolated from the very allies it needs" (statement of November 2007, as cited by the Statewatch "Observatory on Data Protection in the EU" (retrieved from http://www.statewatch.org/eu-dp.htm).

It is the merit of Rey Koslowski of the University at Albany, a well-reputed expert on border control and homeland security in the information age and a frequent witness in this matter at US Congressional hearings, to have pointed to a surprising link between the well-known toughness of US border policies and a less well-known inefficiency in establishing alternative control mechanisms within the US territory.

For Koslowski, Europe has much less of a need for a stringent border system as EU countries "strictly enforce their migration laws within their countries, while there is very little internal enforcement within the US".[93] This can easily be explained by the fact that in most EU member states, legal immigrants as well as European citizens routinely register with the police when they move to a new address and carry ID cards that the police may ask to see at any time. There are also checks at the workplace, work permits are required and enforced, and employers will be tightly controlled. By contrast, once migrants have crossed the border in the US they will rarely be stopped any more.

In the US – as well as in practically all other common law countries – it has not been possible, despite several attempts by the Bush administration, to launch a halfway promising campaign in favour of a national ID card. Irrespective of good factual arguments (several of the 9/11 hijackers were able to board the plane although they did not have a valid ID) the population traditionally rejects the concept of ID cards to such an extent that politicians seem to shrink away from any further attempts (see Box 3).

Box 3. The ID card issue

The specific ID-card sensitivity of the US population as well as other common law countries seems to be founded on a deep sense of mistrust towards all kinds of central authority, even their own governments: for some, ID cards represent an evil per se, a "symbol of a 'papers-please' society reminiscent of Nazi Germany and Stalinist Russia".[†] There is even suspicion over a legislative bill to introduce national driver's licenses because they might "result in a national ID card that compromises privacy" – six US states have already rejected the federal project and it seems unlikely to be realised.

[†] These comments are attributed to Neal Kurk, the Republican State Representative from New Hampshire in a *USA Today* article of 18 June 2007 (as reported by Frank, 2007). Similar statements are available in great numbers from other parts/groupings in the US and Canada.

Source: Frank (2007).

Although emotions have not seemed quite as heated as in other common law countries, Canada still does not possess a national ID card either (CIPPIC, 2007). Makeshift solutions in order to facilitate travel and other domestic affairs, e.g. to open a bank account or provide proof of residence include a combination of official and private documents, such as driver's licenses, birth certificates and electricity bills (Munroe, 2008; CIPPIC, 2007). It is interesting to see that the scepticism of the Canadian public towards the national ID card also has to do with its "low reliability due to a high falsification risk"; surprisingly enough, they do not see the same risk with other official or private-sector cards (ibid.).

The lesson to be retained would thus be that borders are not the only place to control migration and its negative side effects in terms of transnational crime and terrorism. While it is obvious that migration and crime control by means of an ID card mechanism is not everyone's preference and that there are strong traditional objections to such an approach in the Anglo-Saxon/common

[93] See Koslowski (2006), p. 92.

law world, international discussions should take into account that the difficulty of coming to grips with efficient measures against illegal migration and terrorism has to do with not just one but two sensitivities – evenly spread over both sides of the Atlantic!

2.2.2 The (so far) just one-sided benefits drawn from passenger data

When speaking about some unbalanced risk distribution in terms of sensitivities, the same may be true regarding the benefits drawn from the PNR and related mechanisms.

Even though the PNR concept originally stems from the North American toolset, one might imagine that after so many years of intense cooperation the EU would have installed its own set-up to take advantage of a system that runs anyway and produces data that could be retrieved with a simple snap of the fingers. The EU is not yet ready for it, however, even though the US has promised reciprocity in its Undertakings under the 2004 Agreement.[94]

So far, the EU has confined its legislative action more or less to rendering the PNR requests by other countries compatible with EU concepts in data protection.[95] In 2007, for the first time, the Commission extended its scope of reflection to include an EU scheme for exploiting PNR data. The Commission proposal in question is still under consideration at the Council and European Parliament levels.

Although – given the current trend towards tighter security approaches in Europe – it can be expected that the **EU PNR scheme** will be operational in the not too distant future, an attentive observer of PNR history will have noticed another imbalance in transatlantic negotiations.

The entire transatlantic negotiation round started in 2002 as an emergency measure when European airlines were confronted with the urgent choice of either facing heavy fines/loss of US landing rights (when not complying with the new US PNR rules)[96] or infringing EU data protection laws as laid down in Directive 95/46/EC.[97]

The threat of losing access to American airports has continued to accompany the transatlantic PNR negotiations ever since that time. One cannot exclude that certain clauses accepted by the EU negotiators and later on bitterly criticised by privacy commissioners would not have been reconsidered/renegotiated if the EU had been somewhat more at ease in these circumstances.

The question many observers have raised with astonishment is why the EU has shown and still shows such unease and haste about quickly coming to terms with the US?[98] In reality, the EU is not at all deprived of its bargaining power, since in conjunction with the member states it could always retaliate by equally withdrawing landing rights to US airplanes. It has been feared, however, that retaliation measures of such a fundamental nature would not be understood by the European citizens who want – according to a somewhat suspect assumption – above all to enjoy continued and unimpeded travel to the US.

---

[94] See para. 45 of the Undertakings of the DHS–CBP of 11 May 2004 in the Annex to Decision 2004/535/EC (European Commission, 2004).

[95] This approach had already been adopted by the first official statement in terms of the Commission Communication of December 2003 (European Commission, 2003). Yet, as regards the biographic data, under the API scheme the Directive 2004/82/EC has authorised member states to request such data from airlines and run it against JHA databases such as the SIS (see Council of the European Union, 2004).

[96] See the Enhanced Border Security and Visa Entry Reform Act of 14 May 2002.

[97] See European Parliament and Council of the European Union (1995).

[98] This attitude was noticed with astonishment even by the US side, e.g. by Jonathan M. Winer, former US Deputy Assistant Secretary of State International Law Enforcement (Winer, 2006, p. 122).

The same psychological mechanism plays within the closely related area of the US VWP and its conflict with basic features of the EU visa policy: again, the EU has adopted a somewhat half-hearted negotiation style that handicaps the successful implementation of a confirmed EU policy position.

According to the solidarity provision of Art. 1(4) Regulation (EC) No. 539/2001,[99] member states exposed to a visa requirement by a non-EU country may invoke the solidarity of all the others to the effect of introducing a general EU visa requirement for the citizens of that state in return. When this situation occurred in 2004 for most of the new EU member states, Brussels hesitated to go beyond verbal protestations towards the US delegation, while simultaneously discouraging the member states concerned from making use of the solidarity clause.[100] It also seems that in this case the maintenance of a doubtful status quo was more important than defending accomplished EU positions. The central argument was again that the European public would not understand/approve the use of such a sharp retaliation measure.

It is certain that this strategy did not pay off: neither did the US honour the modest EU approach of not putting at risk the continuity of transatlantic travel, nor did the member states concerned forever want to tolerate such a disadvantaged situation. The consequences became visible in early 2008 when the US announced bilateral negotiations with the non-VWP member states to push through its new PNR requirements in return for a (possible) admission of the 'willing' to the VWP. In defiance of the Commission's call for Union discipline, the Czech Republic and others immediately declared their interest in such arrangements, finally yet importantly because they had been left alone by the Commission in the earlier phases of the VWP struggle.[101]

It would appear important for the EU negotiators to recognise that defending European convictions in the PNR and other negotiations openly and right from the start would produce better results than a partial abandonment of positions in view of some assumed reactions by the 'European public'. In the end, why should the European population suffer more from such disruption than the Americans should? The answer to this question remains open and it is definitely not worth abandoning a good negotiation argument for it.

2.3 PNR and resistance to excessive intrusion

Although the term 'resistance' alludes to times of foreign occupation and totalitarian regimes, it has become more and more common in recent years to describe an attitude towards a growing tendency of "replacing the law [through] counter-terrorism practices across states" (Bigo, 2006). Resistance in this sense takes place not in a clandestine fashion, but by individuals and organisations that in one way or another take part in legislative decision-making, in implementing and applying existing legislation or in shaping public opinion.

One has certainly to distinguish various types of opposition: in some cases, it is a concern of democracy, the rule of law and privacy, while in others resistance may coincide with commercial interests as in the case of airlines that find it an annoying burden to participate in the tightened surveillance of passengers. But it is worthwhile to list all those who object to the current system.

---

[99] See Council of the European Union (2001).

[100] The same situation exists for Greece, which the US authorities have always considered too unreliable to join the VWP (see Siskin, 2005, p. 19).

[101] The Czech Interior Minister Ivan Langer made clear that his country's patience – waiting for EU efforts to bear fruit – had expired: "I'm a free human being in Europe and I'm not a slave of the European Commission" (*EuroNews* of 28 February 2008, retrieved from http://www.euronews.net/index.php?page=europa&article=472497&lng=1).

2.3.1 Government institutions

Regarding the institutions, one can easily identify the **gap between executive and legislative powers**, at least on this side of the Atlantic.

In both the **US and Canada**, the post-9/11 counter-terrorism legislation (US Patriot Act and the Canadian Anti-Terrorism Act) as proposed by governments received almost unanimous support by the respective legislatures,[102] despite serious objections about incompatibility with fundamental rights having been voiced by civil rights groups and other critics. In 2005–06, when the respective Acts had to be renewed, a considerable difference became apparent between the two countries, with US Congress reconfirming the Act with almost the same overwhelming majority as back in 2001, while the Canadian House of Commons clearly refused the renewal of the Anti-Terrorism Act.

Within the **EU**, even governments – despite many avowals of solidarity – were initially hesitant to pick up the pace of change adopted by the US (Hamilton, 2006; Rees, 2006; Spence, 2007), but this eventually started to change, especially after the Madrid and London bombings, which made terrorism a threat more directly felt by the population (Cameron, 2007). With the 2005 Hague Programme, the Prüm Treaty of the same year and its inclusion in the EU framework (2007) and finally the EU Border Package of February 2008 as major milestones on a road to 'seamless security', one can easily see that European security politics have moved away from former ideals. They are rapidly approaching the neighbourhood of US 9/11 concepts.[103]

Legislatures have been more combative in defending civil liberties: the European Parliament challenged the 2004 EU–US Agreement in PNR matters in court for breaches of fundamental rights,[104] commented positively on the draft EU–Canada Agreement[105] and denounced, through a highly critical Resolution of July 2007,[106] the new instrument with the US as "substantively flawed".[107] Additionally, at the member state level, parliaments have remained critical and vigilant, above all the UK House of Lords with its extremely detailed PNR report in preparation for the 2007 EU–US Agreement.[108] Other parliaments have also left indications that they look closely at such proposals and take the trouble to stand up against their governments when they see human rights violations.[109]

---

[102] See the article "USA PATRIOT Act" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/USA_PATRIOT_Act); see also the article "Canadian Anti-Terrorism Act" in Wikipedia (retrieved from http://en.wikipedia.org/wiki/Canadian_Anti-Terrorism_Act).

[103] Such a conclusion may be drawn from statements by national politicians who increasingly tend to 'think the unthinkable' with regard to counter-terrorism, in terms of abandoning established democratic and legal principles, for example the distinction between internal and external security and the presumption of innocence (see *Spiegel Online*, 2007, reporting on some "excursions on dangerous terrain" by German Interior Minister Wolfgang Schäuble).

[104] The European Parliament succeeded insofar as the Agreement was annulled, but for reasons of "ultra vires" and not for the reasons of substance emphasised by the European Parliament (see UK Parliament, House of Lords, 2007, p. 21).

[105] See ePractice.eu (2005).

[106] See European Parliament (2007).

[107] See EurActiv (2007b).

[108] See UK Parliament, House of Lords (2007).

[109] Just to cite two examples, see that for Germany in Deutscher Bundestag (2007) and the Czech Republic in EDRI (2007).

2.3.2 Judiciary

The **judiciary**, which in general counter-terrorism matters has acquired a reputation of courageously defending civil liberties against intrusions by the executive,[110] has earned much less merit in the specific PNR field. The European Court of Justice profoundly disappointed the European Parliament (the plaintiff) in Joined Cases C-317/04 and C-318/04, when its annulment of the 2004 EU–US Agreement was solely founded on "ultra vires" rather than on a breach of fundamental rights.[111] Among the deplorable consequences of the decision, 1) PNR data when used for counter-terrorism purposes no longer benefits from privacy protection under Directive 95/46/EC, but finds itself in a legal void owing to the lack of a third-pillar data protection instrument; and 2) the European Parliament will for the time being "have no formal say in the negotiation of any subsequent agreement" (UK Parliament, House of Lords, 2007, p. 22).

2.3.3 Data protection authorities

The main burden – as always on battlefields of this kind – has been resting on the shoulders of **data protection supervisors** and **privacy commissioners**.

In **Canada**, the federal Office of the Privacy Commissioner (OPC) jointly with colleagues from the provinces achieved a first major success in 2003 by removing a "genuine and unprecedented privacy threat" emanating from the new "Big Brother" database on travel activities as designed by Canadian customs (then the Canadian Customs and Revenue Agency).[112] A second victory for privacy interests was seen in the additional commitments made by the new CBSA in 2005 in the context of the EU–Canada Agreement. Being an executive instrument on the Canadian side and the involvement of privacy institutions thus not compulsory, the achievement is credited to the EU Article 29 Working Party under Directive 95/46/EC, whose opinion[113] was followed in this context.[114] In recent years, efforts to avoid erosions of privacy rights have been less successful, notably in the case of the Passenger Protect Programme/no-fly list of 2007[115] when a joint resolution by all the privacy commissioners was simply not taken into account. The current review of the Privacy Act of 1983 is seen as a test case of the extent to which the privacy commissioners will be able to influence future privacy-related policies.[116]

In the **EU**, the untiring efforts by data protection authorities (DPAs) are documented by at least 15 detailed opinions delivered since 2002 by the Article 29 Data Protection Working Party, which deals exclusively with airline passenger data.[117] This accounts for approximately 10% of the report volume produced by the Working Party and is at the top of the interventions by the European Data Protection Supervisor Peter Hustinx. These opinions and their undeniable impact on policy-making are covered in more detail below in the legal analysis of the respective instruments.

---

[110] An example here is that of the acquittal of 9/11 suspect Mounir al-Motassadeq by the German High Court BGH. For reasons of counter-terrorist strategy, he had been deprived of taking advantage of his full rights under the criminal procedure act – see Brimmer (2006); see also *Spiegel Online* (2004).

[111] See the ECJ judgment of 30 May 2006 (cited in appendix I of this report).

[112] See the OPC (2003).

[113] Refer to Opinion 1/2005 of the Article 29 Working Party (2005).

[114] Derived from the letter dated 5 May 2008 from the OPC (C. Baggaley) to the author.

[115] See section 1.2.3.2 above.

[116] See the Statement by Privacy Commissioner Stoddard of 29 April 2008 (OPC, 2008).

[117] For a complete list of opinions/reports of the Article 29 Working Party see the European Commission's website, DG FSJ, "Documents adopted by the Data Protection Working Party" (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm).

2.3.4 NGOs and others

Besides 'data protectors', it is mainly civil liberties NGOs[118] and monitoring services that contribute to raising public awareness of privacy intrusions. Statewatch, the Electronic Privacy Information Centre (EPIC) and Privacy International maintain specific observatories on airline data.[119]

Airline resistance is mainly inspired by the legitimate interests of trade, to prevent excessive government regulation beyond what is necessary for ensuring traffic safety. They oppose external interference on the content and structure of PNR records, pointing quite convincingly to the financial sector, which has never seen an effort to "impose restrictions on the world's financial institutions to regulate what data can or should be part of that transaction" (ICAO, 2004).

3. Acceptability check: Is the EU–Canada Agreement any better than the controversial EU–US instruments?

Having performed this panoramic overview of airline passenger data and its functions, uses and abuses in current times in the North Atlantic region, it would now be appropriate to look more closely at the individual instruments to see how well they conform to the legal frameworks created at the national and international levels.

All current privacy legislation goes back to the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* of 1980,[120] which – indicating its name and provenance – is not in the first place a defensive instrument in favour of citizens to protect them against privacy intrusions but rather a tool of trade facilitation. Its purpose is to prevent the "danger that disparities in national legislations could hamper the free flow of personal data across frontiers", which in turn "could cause serious disruption in important sectors of the economy, such as banking and insurance" (OECD, 1980, p. 1). Still, the principles established by the OECD, ranging from "collection limitation" to "accountability", seem to please everyone, at least as they allow for some creative interpretation of the rules.

Although all parties claim to start from the same golden rules, it is striking to see how the terminology diverges among the various national and regional implementations of the OECD guidelines: confusion starts within the guidelines themselves, whose section headings are not always representative of what the section contains.

For example, section 7, entitled "Collection limitation principle" also includes fair information elements, i.e. that the person concerned should have given his/her consent to the collection or at least knows about it. Others wishing to adapt the OECD rules to academic or practical purposes have left the principles unchanged but they attach entirely different labels to them (Shimanek, 2001).[121] The most common implementation mode, however, is to 1) redraft the text of the

---

[118] For a comprehensive listing of privacy organisations and other resources, see the EPIC's "Online Guide to Privacy Resources" (retrieved from http://epic.org/privacy/privacy_resources_faq.html#Privacy_Organizations).

[119] Refer to Statewatch's "Observatory on the exchange of data on passengers (PNR) with USA" (retrieved from http://www.statewatch.org/pnrobservatory.htm); see also the EPIC's "EU–US Airline Passenger Data Disclosure" (retrieved from http://epic.org/privacy/intl/passenger_data.html); and also Privacy International's "Travel Surveillance" (retrieved from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559086).

[120] See OECD (1980).

[121] Such labels include 'notice, 'purpose', 'consent', 'security', 'disclosure', 'access' and 'accountability'.

principles, 2) reassign certain elements from one principle to another, 3) modify the names/labels of principles, and 4) completely reshuffle the order of the principles.

Implementation instruments have again found different structures and organisation principles in reproducing the OECD rules[122] – to the extent that the unfamiliar reader often feels left alone, desperately wishing that this 'Babylonian confusion of tongues' be mitigated at least by a table of correspondence linking the various terminologies.

The present report thus attempts to find a pragmatic way to give appropriate weight to the different privacy-related comments and evaluations, no matter whether they are based on OECD, EU, Canadian or other terminologies.

3.1 Identification of appropriate criteria, notably in the field of recognised privacy rules

In view of the numerous approaches available to structure the basic principles of data protection, it seems indispensable to first, opt for a single approach to be applied to all instruments in question in order to ensure comparability, and second, to ensure that this approach be visibly interlinked with the internationally accepted standards.

Given the prominent role of the Article 29 Working Party[123] concerning all the PNR instruments so far discussed or adopted, notably by providing detailed opinions in the various stages of the legislative procedure, it would appear most appropriate to follow their outline in examining the compatibility of the EU–Canada Agreement with universal privacy standards. This would be combined with the provision of a table of correspondence linking the Working Party's scheme with other standard schemes.

The utilisation of its own set of terminology and structure – quite distinct from that used under Directive 95/46/EC – bears the advantage of not having been directly affected by the ECJ decision of 30 May 2006, which declared the Directive inapplicable to enforcement-related PNR matters.[124]

On the Canadian side, the terminology question is equally complicated: the Privacy Act of 1980, still stemming from the pre-OECD period, does not even contain a list of principles, while such a list is available in the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000, but formally the latter Act only applies to private-sector data issues. In practice, Canadian privacy commissioners loosely refer to fair information principles and practices and global privacy standards[125] as accepted at the international level.[126] Furthermore, Canadian privacy experts have become broadly familiar with the EU nomenclature – especially since the

---

[122] Clarke (2000, ss. 2.4 and 2.5) attributes this to different approaches ranging from conventional "fair information practice" policies with an emphasis on the protection of *data* (rather than the persons concerned) to those based on the recognition of a "fundamental human right" (e.g. Art. 1(1) of Directive 95/46/EC).

[123] See the Working Party under Directive 95/46/EC 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 (European Parliament and Council of the European Union, 1995).

[124] See the 2006 ECJ judgment cited in appendix I of this report.

[125] See the 28th International Conference of Data Protection and Privacy Commissioners (2006).

[126] Ibid.

Article 29 Working Group, with its opinions, exercised a decisive influence on the outcome of the EU–Canada PNR negotiations.[127]

The standard examination scheme employed by the Article 29 Working Party – as referred to in Opinion 3/2004[128] – implies the following elements:

a) Data protection should be recognised as a fundamental right to the end that any restriction imposed must be carefully weighed to find a balance between security concerns and the civil liberty at stake (Article 29 Working Party, 2004).

b) Due regard should be given to the transitional character of adequacy findings – in view of rapidly changing threat scenarios in the case of terrorism and transnational crime, data flows should not be authorised for an undetermined period but made subject to a sunset limitation.

c) Basic data protection principles should be applied ("content principles") as set out below.[129]

i) Purpose limitation principle

Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer.

ii) Data quality and proportionality principle

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

iii) Transparency principle

Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness.

iv) Security principle

Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

v) Rights of access, rectification and opposition

The data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations, s/he should also be able to object to the processing of the data relating to him/her.

---

[127] Derived from the letter of 5 May 2008 from the Canadian OPC (C. Baggaley) to the author, underlining the importance of the Article 29 Working Party's Opinion 1/2005, all the more as the OPC was not invited to participate in the negotiations.

[128] See Article 29 Working Party (2004), s. 2.

[129] Refer to Article 29 Working Party (1998), p. 6.

vi) Restrictions on onward transfers

Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.

d) Procedural/enforcement mechanisms should be in place that provide[130]

i) a good level of compliance with the rules;

ii) support and help to individual data subjects; and

iii) appropriate redress to the injured party.

3.2 Evaluation of the EU–Canada Agreement of July 2005

The 'model' among PNR instruments with its strikingly "good balance between security requirements and the data protection standards"[131] is the result of close scrutiny exercised by the EU data protection authorities, as can well be evidenced by comparing the Agreement text at its various states of development (see Box 4).

Box 4. Various comments on the EU–Canada Agreement

The Article 29 Working Party delivered two detailed Opinions (3/2004 and 1/2005) on the level of protection granted to PNR data in Canada in addition to an opinion by the European Data Protection Supervisor on the proposed agreement as such (EDPS, 2005a). Meanwhile, other bodies have confined themselves to very meagre contributions: the European Parliament rejected the Agreement for the formal reason that the new instrument should not be concluded before the outcome of the ECJ procedures on the EU–US instrument was known (European Parliament, 2005). MEPs conceded, however, that content-wise the Agreement represented an "acceptable balance" (ibid.).

The initial comments on the Canadian adequacy situation in PNR matters were still rather critical – hardly different from those issued on previous EU–US negotiations – but the tone changed decisively with the progress of negotiations between the Commission and Canadian authorities and the improvements conceded by the customs/border authorities.

3.2.1 Data protection as a fundamental right

The reference to the fundamental rights character is a reminder that privacy is not just any 'lightweight' position within the EU legal order, but on the contrary is an important pillar of the legal order that may be subject to restriction only if a similarly important interest is at stake (Article 29 Working Party, 1998).

In the case of the PNR, the value at stake is the 'fight against terrorism', which is routinely accepted as a sufficiently developed counterweight since it represents "both a necessary and valuable element of democratic societies" (Article 29 Working Party, 2004). Yet in this context, terrorism does not stand on its own, it is combined – just as in the case of the 2004 EU–US

[130] Ibid., p. 7.

[131] See ePractice.eu (2005).

Agreement – with the much wider field of "terrorism-related and other serious crimes, including organised crime, that are transnational in nature".[132]

This position is in sharp contrast to the Commission's Decision 2006/253/EC on the adequate protection of personal data transferred to the CBSA (henceforth 'Adequacy Decision'), which solely refers to the Community's "commitment to supporting Canada in the fight against terrorism".[133] Surprisingly, not even the normal watchdogs (the Article 29 Working Party or the European Data Protection Supervisor (EDPS)) take any offence at this – neither at the divergence between the adequacy finding and the actual Agreement text, nor at the diffuse concept of "terrorism-related and other serious crimes", which leaves room for a wide spectrum of interpretations.[134]

In its first Opinion (3/2004), the Article 29 Working Party still expressed serious doubts as to these "too widely defined purposes" (Article 29 Working Party, 2004, s. 6), but dropped this charge in early 2005, without any significant amendments having been made to the text.[135] Only the UK House of Lords (2007, paras. 104*f.*) remained sceptical of the delicate aspects of this formula, which by now seems to have acquired the status of an EU standard clause, as contained in the US Agreements of 2004 and 2007 as well as in the proposal for an EU PNR system of 2007.[136] This situation leads to the simple question, "[H]ow serious must a crime be to fall within this description and so be covered by the PNR Agreement?" (UK Parliament, House of Lords, 2007).

As there is presently no internationally agreed definition of 'serious crimes' (nor 'terrorism-related crimes'!), the formula chosen raises considerable doubts not only under the fundamental rights aspect but also under that of purpose limitation and onward transfer. Crimes other than terrorism are likely to bring in entirely different sets of authorities concerned, which will in turn widen the scope of those accessing the data in question (see section 3.2.3.6 below). At this stage, the question should be kept in mind as to whether a positive list of 'serious crime' categories (loosely inspired by the model of the European Arrest Warrant)[137] should be agreed – best at a multilateral level – to avoid grave inconsistencies in international privacy protection.

3.2.2 Transitional character of the adequacy finding

Data protection supervisors warn that adequacy findings are not made for eternity: they represent a snapshot of the current state of foreign privacy legislation, which is clearly subject to change (EDPS, 2005a, para. 10). Besides the option of an ad hoc suspension of data flows in the case of major changes, any such arrangements should be time-limited (Article 29 Working Party, 2005, s. 3). This is best done by means of a sunset limitation bringing the adequacy finding and thus the agreement to an automatic end if not renewed within a given time period (Article 29 Working Party, 2004, s. 3).

---

[132] Refer to the EU–Canada PNR Agreement (2005), 1st recital.

[133] See European Commission (2005b), 8th recital.

[134] Refer to the Article 29 Working Party (2004 and 2005), as well as EDPS (2005a).

[135] See Article 29 Working Party (2005), s. 3.

[136] See European Commission (2007a).

[137] Refer to the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (Council of European Union, 2002).

The 2005 Agreement fully complies with this requirement by foreseeing 1) in its Art. 5(2) that the obligation of air carriers to transmit PNR data to Canadian authorities ceases to exist with the expiry of the Adequacy Decision, and 2) in Art. 7 of the Adequacy Decision that the Decision expires after 3.5 years if not extended beforehand.

A continuous monitoring of the Agreement and its operation is ensured by the Joint Committee under Art. 6 of the Agreement, which is in charge of settling possible disputes (Art. 7) and organising the joint reviews (Art. 8).

3.2.3 Compliance with content principles

Compliance with the standard data protection principles, as specified under section 3.1 above, is seen as discussed below.

3.2.3.1 Purpose limitation

Both the European Commission and EU data protection authorities have positively expressed their satisfaction that the PNR data transferred from EU air carriers to the CBSA will be "processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. In particular, PNR data will be used strictly for purposes of preventing and combating: terrorism and related crimes [along with] other serious crimes, including organised crime, that are transnational in nature."[138]

Doubts remain, however, about the extent to which such a wide formula may be considered an effective 'purpose limitation': one might just refer to the initial comments by the Article 29 Working Party, with the criticism that

> these purposes are too widely defined, and in particular go well beyond the purpose of fighting acts of terrorism. Automatic access by customs and law enforcement authorities to personal and commercial data contained in airline passengers' information constitutes an unprecedented derogation to the right to collect data for commercial purposes and should only be justified on the basis of very serious concerns.[139]

Between the first and the second intervention by the Article 29 Working Party, the original text was amended only insofar as the transnational element was added as a further condition for the use of PNR data. This, however, changes nothing about the ambiguity of the term 'serious crimes' for which the Canadian authorities wish to use PNR data; it is therefore hard to understand where the sudden satisfaction of the Article 29 Working Party stems from. Neither have the Canadian authorities delivered the "clear and limited list of serious offences directly related to terrorism" required by the Working Party nor have they provided any confirmation that the serious crimes at stake have a "clear relationship with terrorism".[140]

3.2.3.2 Data quality and proportionality

As with most categories, comments are broadly positive regarding the data quality and proportionality criterion. When the Commission's Adequacy Decision claims full success in all major items negotiated with the Canadian authorities, it meets no opposition by data protection authorities (not even by civil liberties groups!).

---

[138] See European Commission (2007a), 15th recital; see also the Article 29 Working Party (2005), s. 3; and also EDPS (2005a), s. 4.3.

[139] See Article 29 Working Party (2004), s. 6.

[140] See the Commitments by the CBSA in the Annex to Decision 2006/253/EC (European Commission, 2005b), s. 2.

Limited list of categories[141]

The particularly lengthy list of 38 data categories[142] initially required by the CBSA was reduced to 25, more specifically by eliminating so-called 'open categories' that could reveal sensitive information on the passengers. Remaining doubts by the EDPS concerned categories 10 (frequent flyer information) and 23 (APIS information), as such data could still concern sensitive aspects of behaviour – but were considered "not serious enough to require renegotiating the Agreement" (EDPS, 2005a, s. 4.2).

Transmission solely through the push method

A major achievement was the exclusive adoption of the push method, thus allowing airlines to keep control over the data transfer.[143]

Enhanced data quality

Finally yet importantly, as a result of their own painful experience (see the Maher case),[144] the Canadian authorities subscribed to two crucial commitments, i.e. 1) to apply no change to the PNR data obtained, and 2) to collect additional data to supplement PNR data only through lawful channels (European Commission, 2005b, 16th recital). Such precautions help to avoid major errors in the targeting of suspects (so-called 'false positive hits'), which are mainly attributed to the poor data quality of enforcement databases and watch lists.

Reduced retention periods

While approving in principle the Canadian system of graded access during successive retention periods (in 0-72 hours, direct access to the full name record by customs/immigration officers; from 72 hours to the end of 2 years, name anonymised towards most officials except intelligence officers; from 3 years to the end of 6 years, the personalisation data is accessible only in very exceptional cases), the Article 29 Working Party objected to the "rather long" period during which personalised data items remained accessible. Data should remain personalised only during the initial period following entry into the territory (Article 29 Working Party, 2004, s. 5.5).

After considerable concessions by the CBSA, the maximum retention period was reduced from 6 to 3.5 years, with the name data being accessible after the initial 72-hour period only in very exceptional circumstances.[145]

3.2.3.3 Transparency

As a primary element of transparency, the Article 29 Working Party requested the Commission to include a "full picture of the relevant Canadian regulatory framework…as an annex to the Commission Decision" (Article 29 Working Party, 2004, s. 5). Although this formal requirement was not complied with, a concise description of the Canadian regulatory framework is contained in the Working Party's Opinion 3/2004 (see Box 5).

---

[141] Refer to Annex II of the Agreement (EU–Canada, 2005).

[142] This is a list "well beyond what could be considered adequate, relevant and not excessive", according to the Article 29 Working Party (2004), s. 6.3.

[143] See the Commitments by the CBSA in the Annex to Decision 2006/253/EC (European Commission, 2005b), s. 7.

[144] For details on the Maher case, see section 1.1.2.1 above.

[145] See the Commitments by the CBSA in the Annex to Decision 2006/253/EC (European Commission, 2005b), s. 8.

Box 5. The Canadian regulatory framework

In basic terms, the API/PNR programme was set up in 2001 by the predecessors of the CBSA under the Customs Act (Bill S-23) and the Immigration and Refugee Protection Act (IRPA). Section 107.1 of the Customs Act together with section 148(1)(d) of the IRPA allowed the government, by means of the Passenger Information (Customs) Regulations, to require the provision of API/PNR data prior to arrival in Canada. The IRPA as amended by Bill C-17 allows for information-sharing arrangements with other Canadian agencies.

Sources: Article 29 Working Party (2004), s. 5; for the Canadian legislation cited, see appendix I of this report.

Under the auspices of transparency, the CBSA also committed itself to provide information to travellers concerning the purpose of the transfer and processing, and the identity of the data controller.[146] Furthermore, the Commission's Adequacy Decision provides clear instructions as to the circumstances under which the data flow to Canada is to be suspended by member states (European Commission, 2005b, Arts 3 and 4).

3.2.3.4 Security

EU data protection authorities excel in praising the technical and organisational security measures taken by Canadian authorities[147] in order to avoid data leakages. There has been no complaint in this regard (EDPS, 2005a, s. 2).

3.2.3.5 Rights of access, rectification and opposition

While the Canadian system of providing *redress procedures to data subjects* has been considered exemplary right from the start, initial criticism sharply denounced the exclusion of foreigners not resident/present in Canada from this mechanism (EDPS, 2005a, s. 2). The CBSA has therefore agreed, in section 31 of the commitments, to allow EU residents to initiate a complaint through their national data protection authorities, which was considered a satisfactory solution (Article 29 Working Party, 2005, s. 3.6.1).

It is underlined by the EU data protection authorities that the agreed redress procedures – just as all the other commitments made by the Canadian authorities – are based on *legally binding engagements*, which distinguishes them positively from similar arrangements taken with the US (EDPS, 2005a, s. 4.1, 18). In addition, Canadian legislation provides for criminal and other sanctions in the event that the commitments are not respected. Finally, the privacy commissioner is empowered under the Privacy Act to commence an investigation in respect of the disclosure of personal information.[148]

3.2.3.6 Restrictions on onward transfers

The issue of onward transfers as regulated by the CBSA again meets with full approval by the EU DPAs,[149] since according to the commitments 1) transfers/disclosures will never be made in

[146] See the Commitments by the CBSA in the Annex to Decision 2006/253/EC (European Commission, 2005b), s. 12.

[147] Ibid., s. 33*ff*.

[148] Ibid., s. 35.

[149] See Article 29 Working Party (2004), s. 6.5; see also Article 29 Working Party (2005), s. 3.5; and also EDPS (2005a).

bulk but decided on a case-by-case basis, 2) there will be no online access granted to other authorities and 3) disclosures will depend on the conditions that a) they are relevant to the other agency, b) they respect the purpose limitation referred to under 3.2.3.1 above, and c) the recipients undertake to afford it the same protection.[150] Similar safeguards apply to the disclosure to other countries.[151]

The only doubt that remains over this perfect construction concerns the imprecise purpose limitation that we have already denounced under section 3.2.3.1 above. Vague terms such as 'serious crimes', with their strong risk of diverging interpretations, are quite likely to hamper the effective protection of privacy interests, especially when data flows occur at the international level.

3.2.4 Procedural/enforcement mechanisms

Although most of the procedural items have already been touched upon in connection with the content principles, a few references should be made.

3.2.4.1 Good level of compliance with the rules

The existence of mechanisms ensuring a high level of compliance has been extensively appreciated by the EU DPAs, for a number of reasons: 1) the advanced technical and organisational security measures referred to in section 3.2.3.4 above, 2) a refined system of redress available to citizens concerned, 3) legally binding commitments subscribed to by the Canadian authorities combined with criminal and other sanctions in case of infringements, and 4) the independent role of the privacy commissioner serving as a watchdog over compliance with the law (refer to section 3.2.3.5 above).

3.2.4.2 Support and help provided to individual data subjects

Citizens benefit from the general transparency principle, which requires the authorities to advertise 1) the fact that passenger data is being collected as well as 2) the reasons for doing so and 3) finally the possibilities of redress granted under the Privacy Act. An important support function has been entrusted to the privacy commissioners at the national and provincial levels, who may independently examine cases of possible infringements to the privacy rules (refer to sections 3.2.3.3 and 3.2.3.5 above).

3.2.4.3 Appropriate redress provided to the injured party

The Canadian redress procedures – generally considered fully appropriate – are described in more detail in section 3.2.3.5 above.

In conclusion, it can be said that the EU–Canada Agreement to a large extent lives up to the high expectations nourished by the numerous positive reviews it has received in recent years, mainly in comparison with agreements signed on the same subject with the US. Aside from the minor digression from the 'path of virtue' in terms of the somewhat imprecise description of the purposes pursued by the Agreement, the text truly confirms its reputation of a well-crafted instrument that takes up its responsibility to protect citizens to the utmost degree from undue privacy intrusions that may occur during the operation of PNR mechanisms.

---

[150] See the Commitments by the CBSA in the Annex to Decision 2006/253/EC (European Commission, 2005b), s. 12*ff*.

[151] Ibid., s. 16*ff*.

3.3 Comparative overview of other major PNR instruments[152]

A comparison between the EU–Canada Agreement and other recent instruments gives additional clarity as to the quality of this flagship instrument; it also contributes to identifying the current tendencies in revised PNR concepts – possibly a signpost to where the forthcoming EU–Canada negotiations will lead.

3.3.1 The EU–US Agreement of 2004

Turning away from Canada and looking at the EU agreements with the US, one quickly becomes aware that this is another category of international cooperation: the contrast could hardly be more striking even at first sight.

The EU–US instruments already stand out by the sheer number of critical comments they have attracted. This may have to do with the scrutiny to which US action at the international level is traditionally exposed. Nevertheless, such scolding does not exclusively come from those who frequently pinpoint US human rights violations in the context of Iraq, FBI/CIA intrigues or the Guantanamo/Abu Ghraib prisons. There also are highly reputed bodies such as the UK House of Lords EU Select Committee, which gives a strong warning against undesirable trends developing in PNR negotiations with the US.[153] They are part of a much larger group of public institutions, data protection authorities and media whose statements, warnings and protests including judicial action have accompanied the entire history of EU–US negotiations and arrangements.

If it is true that in the case of Canada, the public hardly took note of the event and even public bodies spent a minimum of paper in order to deliver their – mainly well-received – comments, the opposite applies to the US negotiations. Especially the data protection authorities have lavished the negotiation parties with good advice and admonition – and have been regularly disillusioned to see that their detailed opinions had all had been in vain. The European Parliament, after its objections against the Commission's adequacy finding had not been accepted, saw no other way out than to challenge the relevant Commission and Council decisions. Civil liberties organisations such as Statewatch, the EPIC and Privacy International, which remain practically silent on the EU–Canada Agreement, dedicate entire 'observatories' to EU–US airline passenger data disclosure.

This peculiar situation might best be explained by the heated atmosphere in the aftermath of 9/11: the transatlantic divide in the search for appropriate solutions in tackling terrorist threats had its repercussions down to the details of airline passenger control. The 'war' (as opposed to the 'fight') against terror, as seen by the US side, justified the use of uncommon means: at the latest by July 2003, the US had removed the separation ('wall') between information obtained by the law enforcement and intelligence communities (Rees, 2006, p. 82). This also allowed a wider choice of options when looking at details of airline security risks. Europeans felt irritated not

---

[152] Owing to time and space constraints, this report confines itself to an examination of the transatlantic instruments. Other texts on the international/regional levels would be interesting to look at, but in most cases they have not yet reached the status of adoption or at least advanced preparation (e.g. the proposal for an EU Framework Decision of 2007 and planned EU–Australia and EU–Korea agreements). The only text fully operational is the 2005 MoU between Canada and Switzerland, which follows similar orientations as that for the EU and Canada.

[153] Refer to the statement by Lord Wright of Richmond, Committee Chairman, of 13 June 2007, according to which the new PNR Agreement should be clear, unambiguous and not allow the US to amend the undertakings unilaterally (see the CEPS CHALLENGE article, "Lords EU Committee Raise Concerns over Passenger Name Record Agreement with US", 13 June 2007 (retrieved from http://www.libertysecurity.org/article1489.html).

only by the greater ease in restraining civil liberties and "breaking with democratic traditions" (Cameron, 2007) but also by the rapid change of strategies in such a sensitive area.

European suspicion was particularly fed by subsequent discoveries that – while official negotiations were still in progress – US authorities had already been working on system changes incompatible with the results so far obtained (e.g. exploitation of PNR data by targeting devices such as CAPPS II, ATS and Secure Flight).[154†] Negotiators were puzzled that the US delegation repeatedly came back with imprecise treaty language, blanket clauses and so forth, which are inadmissible in terms of data protection (purpose limitation principle). Even the official European Commission report on the joint review of the 2004 Agreement complained that access to certain control records had been restricted by the DHS for reasons of secrecy (European Commission, 2005, p. 6).

In view of the volume of controversial aspects, the following review confines itself to those that are essential for enabling a comparison with the EU–Canada Agreement.

The compliance problem of the 2004 US Agreement and the degree of its divergence from the EU–Canada instrument may also be illustrated in a quantitative manner: with regard to the 21 criteria applied by the Article 29 Working Party to check privacy compliance, commitments by the US side[155] failed to comply with the rules in roughly two-thirds of the items (14.5 = 66%).[156] By way of comparison, the Canadian commitments had been deemed appropriate in practically all areas with a low failure rate of just 1.5 (= 7%) items of non-compliance.[157]

Major items of concern are set out below (following the order of section 3.2 above).

Item 1. Data protection as a fundamental right

Privacy protection as a fundamental right may be restricted only if an interest of a similar value is at stake. Such a balance of values may be assumed for counter-terrorism but not for the second purpose cited, i.e. "preventing and combating of…other serious crimes", which is considered "too vague" to be acceptable as a description of purposes (Article 29 Working Party, 2004a, s. 5B).

Item 2. Transitional character of the adequacy findings

Formally, there is compliance with this item: 1) there is a 'sunset clause' to terminate the Adequacy Decision/Agreement if it is not renewed within a delay of 3.5 years. 2) Joint reviews to detect possible malfunctions are foreseen on a regular basis according to section 5 of the 2004 EU–US Agreement. 3) In the case of malfunctions, member states may suspend the data flow according to Art. 3 of the Adequacy Decision (European Commission, 2004).

On the practical level, however, the first joint review held in 2005 revealed a number of obstacles to satisfactory verification of data routines, notably related to 1) certain records being denied to the review team for reasons of secrecy and 2) the technical impossibility for the US CBP to identify complaints/requests relating to EU PNR data (European Commission, 2005; Guild & Brouwer, 2006).

---

[154] See section 1.2.3.1 above.

[155] See the Undertakings of the DHS–CBP of 11 May 2004 in the Annex to Decision 2004/535/EC (European Commission, 2004).

[156] This refers to the final comments by the Article 29 Working Party (2004a) as laid down in Opinion 1/2004.

[157] The calculation is based on compliance with the list of privacy criteria displayed in section 3.1 above.

Item 3. Compliance with content principles

Item 3.1 Purpose limitation

The lack of unambiguous purpose descriptions is criticised at various instances: besides the imprecise term of 'serious crimes' – which as a minimum would have required an explanatory list of crimes concerned – there is the intended use of PNR data for unspecified "law enforcement purposes" (Article 29 Working Party, 2004a, s. 5E).

Furthermore, the Working Party points to the following blanket clause-types of inadequacies in the description of purposes:

- the lack (still) of an available list of the agencies authorised to receive data by means of onward transfer;
- a blanket clause allowing the CBP, in its discretion, to forward data to any authorities, including foreign ones, with "law enforcement functions";[158] and
- a blanket clause permitting data transfer "as otherwise required by the law" (ibid., s. 35).

Specifically harsh criticism was given to the undeclared use of PNR data for mass data processing under targeting/profiling systems such as CAPPS II or similar programmes – such systems, being qualitatively different from the mere transfer of passenger data, required additional consideration and specific safeguards (Article 29 Working Party, 2004a, s. 3).

The EU authorities again became concerned about the delicate aspects of such mass data processing, when they were confronted by the existence of yet other profiling and targeting systems such as ATS and Secure Flight whose existence had not even been revealed to the joint review team.[159]

Item 3.2 Data quality and proportionality

List of data categories

The final list of 34 data categories found no approval by Article 29 Working Party: it was considered excessive since so far, only four *acceptable* categories had been eliminated from the original proposal, while sensitive items such as OSI and SSRs containing information on special needs/preferences of passengers remained on the list (Article 29 Working Party, 2004a, s. 5C).

Transmission through the push method

The outdated pull method allowing the CBP to access airline computers and pull out the data needed remained in place wherever airlines were not yet ready for the new system. The technical possibility of roaming around on such computers and obtaining an excessive amount of data was solely balanced by a commitment that the CBP would avoid pulling/using sensitive data and would delete such data where accidentally pulled.[160]

Contrary to initial intentions, the US side had done very little to replace the former pull method with the privacy-compliant push system: the EU review team even assumed that the CBP had the intention "to retain some sort of a pull system" (European Commission, 2005, p. 1).

---

[158] See s. 29 of the Undertakings of the DHS–CBP in the Annex to Decision 2004/535/EC (European Commission, 2004).

[159] See the American Civil Liberties Union (2007).

[160] See Article 29 Working Party (2004a), s. 5D; see also the Undertakings of the DHS–CBP in the Annex to Decision 2004/535/EC (European Commission, 2004), s. 9.

Data quality

Deficiencies regarding data quality were seen in the fact that 1) the access to sensitive data was insufficiently blocked (e.g. by use of the pull method) and 2) that the "use of trigger words" to eliminate such data represented an inept solution (Article 29 Working Party, 2004a, s. 5D).

A further data quality problem resulted from matching operations conducted between PNR data and – frequently error-prone – search lists such as CAPPS II (ibid., s. 5L).

Retention periods

The reduced retention period of 3.5 years (instead of 7 years as initially proposed) was welcomed but not accepted as a definite solution. Even the new period is "considerably longer than the weeks or months" that may be considered acceptable, and the additional period of 8 years for manually accessed records was just "disproportionate" (ibid., s. 5F).

The Working Party (at this stage) was not even aware of the effect, in terms of retention periods, of the processing of PNR data by the ATS: in this case, retention was prolonged to 40 years!

Item 3.3 Transparency

The Working Party considered the CBP's plans for informing the travelling public, through a standard notice, of the collection of PNR data and related issues as a sufficiently clear method of complying with the transparency principle (ibid., s. 5J.1).

The further issue of a complete description of relevant US legislation to be displayed in the annex of the Agreement/Adequacy Decision was not raised here (with the Working Party taking a different stance in this instance from their discussion of the EU–Canada Agreement).

Item 3.4 Security

No specific remarks were made under this heading; however, the multiple interlinking of PNR processing with other procedures (e.g. profiling and targeting) suggests that there may be weak links and loopholes that put at risk the security of the entire system.

From an organisational point of view, the fact that the CBP officers were without guidance as to the notion of "serious crimes that are transnational in nature" (European Commission, 2005, p. 2) casts a negative light on the secure and reliable functioning of the programme. Similarly, the system contained no device to identify instances of manual review by CBP officials, which had been authorised solely for exceptional cases (ibid.).

Item 3.5 Rights of access, rectification and opposition

In contrast to the information aspect, access, rectification and redress procedures are regulated in a less satisfactory manner. The system suffers from various exemptions under the Freedom of Information Act (1966), which may work against the data subject when the latter seeks access to his/her own record – in particular when the disclosure would "interfere with the enforcement procedures" or "disclose techniques or procedures" employed by the system.[161]

Rectification under the 1974 Privacy Act is still reserved to US nationals and residents, whereas it is uncertain whether the administrative rectification procedure proposed by the CBP (ibid., s. 39) will work in practice (Article 29 Working Party, 2004a, s. 5J.3)

[161] See the Undertakings of the DHS–CBP in the Annex to Decision 2004/535/EC (European Commission, 2004), s. 38.

Redress procedures as proposed by the CBP were welcomed by the Working Party, which at the time expressed doubts about whether the 'in-house' procedure involving the DHS chief privacy officer as the last point of intercession, even regarding complaints against his/her own office, really represented an appropriate solution (ibid., 5J.4).

Item 3.6 Restrictions on onward transfers

According to the Working Party, serious shortcomings in the area of onward transfers concerned mainly 1) the absence of a list of public bodies entitled to receive the data, and 2) the aforementioned **blanket clauses in sections 29, 34 and 35 of the CBP Undertakings**, which give wide discretion in overriding the principles governing privacy protection in general and in the present Agreement in particular.

Accordingly, the CBP may, in its discretion, forward PNR data to government authorities (including foreign ones) "with **counter-terrorism or law enforcement functions**" (s. 29, emphasis added). Nothing in this Agreement impedes the use/disclosure of PNR data 1) for the protection of vital interests of persons, in particular "**significant health risks**" (s. 34) and 2) "in any judicial proceedings or **as otherwise required by law**" (s. 35, emphasis added).

It is certainly no surprise that the Article 29 Working Party, with support from many sides, drew the conclusion that, despite some progress made, the situation in privacy protection encountered "does not allow a favourable adequacy finding to be achieved" (Article 29 Working Party, 2004a, Conclusion).

3.3.2 The interim EU–US Agreement of 2006

After annulment of the 2004 Agreement by the ECJ decision of 30 May 2006, the parties had to act rapidly in order to establish a new instrument compliant with the views of the Court.[162]

Although the challenge from the European Parliament was based on the claim that the Commission's Adequacy Decision and the Council's decision authorising the signature of the Agreement were ultra vires, i.e. in breach of the fundamental principles of Directive 95/46/EC, in breach of fundamental rights and of the principle of proportionality, the Court based its decision on the view that the said directive was the wrong legal basis. More specifically, data processing operations for the purposes of public security and in the context of criminal law were excluded from the scope of this first-pillar instrument. It annulled both instruments, without having considered the Parliament's other arguments.

The disappointing effect of this judgment is that PNR data, when used for security purposes, do not take advantage of enhanced privacy protection as offered by Directive 95/46/EC but find themselves somewhere in a legal 'no man's land'. In the absence of the third-pillar data protection instrument that has yet to be accomplished, the only protection may be derived from the human rights norm of Art. 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) (Guild & Brouwer, 2006).

The first phase between termination of the 2004 Agreement (taking effect on 30 September 2006) and the entry into force of the 2007 Agreement (end of July 2007) was governed by an i**nterim EU–US instrument signed on 16 October 2006**. While in the interest of continued transatlantic air traffic the EU agreed to the processing of PNR data "in reliance upon DHS's continued implementation of the Undertakings", they had to accept that "things had changed in

[162] For details on this phase, see UK Parliament, House of Lords (2007), p. 21.

Washington during the last couple of years" and that there were **new conditions added by the DHS** as transmitted by the letter from the DHS Assistant Secretary Stewart Baker of October 2006.[163]

The changes concerned notably the following elements:

- The *Undertakings* of the 2004 Agreement were no longer valid in their original form but had to be read "*as interpreted in the light of subsequent events*" (UK Parliament, House of Lords, 2007, s. 60, emphasis as per the original).
- On the sharing of data with counter-terrorism-oriented agencies in the framework of an information sharing environment (ISE) as required by the Intelligence Reform and Terrorism Prevention Act of 2004, contrary to sections 28–32 of the 2004 Undertakings, PNR data now had to be *routinely shared with ISE agencies*.
- The *PNR elements for transmission under field 11 were extended* (frequent flyer information) to cover all frequent flyer elements such as phone numbers and e-mail addresses, as these "may provide crucial links to terrorism".
- *Access to PNR data was extended* "in the context of *infectious disease and other risks to passengers*" (emphasis added), on the basis of Undertaking 34, whose extensive interpretation appeared justified in October 2006 owing to the risk of avian flu.
- The *3.5 year's retention period was cancelled*. According to the DHS, with the premature termination of the Agreement, the (in their eyes "unacceptably short") retention period was obsolete, even for data transmitted during the validity of the 2004 Agreement. Attentive observers such as the House of Lords EU Committee were "reluctant to believe this of partners who, we are told, have always negotiated in good faith" (UK Parliament, House of Lords, 2007, s. 69).

As an overall reaction, the new US approach, including its one-sided "consultation/amendment" strategy, met with complete lack of understanding by the UK House of Lords: undertakings that allow the party giving them to amend them unilaterally "scarcely deserve the name. No such provision should be included in any future agreement" (ibid., s. 77).

This new approach initiated by the Baker letter seems to set the tone not only for the duration of the interim 2006 Agreement but also the time after. If the 2004 Agreement appeared backward in comparison with the EU–Canada instrument, it is now likely to emerge as a relatively safe and solid text, with a much higher privacy profile than all that comes after. We have to examine the extent to which this assumption applies to the 2007 instrument.

3.3.3 The EU–US Agreement of 2007

At first sight, it is apparent that the **2007 EU–US Agreement** has been stripped of the procedural safeguards in terms of adequacy decisions, the legislative role of the European Parliament and the formal opinions by the Article 29 Working Party and EDPS that had faithfully accompanied the adoption of former PNR instruments. It is certainly worthwhile to retrace the "genesis" of the 2007 Agreement (Guild, 2007) – finally yet importantly to understand why the "successful" court action is rightfully referred to as a "Pyrrhic victory" (Privacy International, 2006), not only for the European Parliament but also for the interests of privacy protection on the whole.[164]

---

[163] The text of the Baker letter is reproduced as Appendix 7 in the House of Lords (2007) report on the EU–US Agreement.

[164] Refer to Guild & Brouwer (2006) concerning the disappointing role of the ECJ in the context of the PNR.

From the very beginning, negotiations were under considerable time pressure since the interim Agreement was definitely to expire on 31 July 2007. The DHS added to this sense of urgency by emphasising that it had no intentions of returning to the former 2004 Agreement and that the former Undertakings would "not [even] constitute a precedent" for discussions on the future agreement (see Undertaking 48 under the 2004 Agreement).

The next surprise arrived in terms of a letter from the DHS to the Portuguese presidency (US DHS letter, 2007), intending "to explain how…DHS handles" PNR matters in general and wishes to handle them with regard to the EU in future (Guild, 2007). It was made very clear that the DHS did not wish to enter into discussions on these practices, but that the EU was just expected to take note of them ("[w]e trust that this explanation has been helpful to you in understanding how we handle EU PNR data"). The EU side replied promptly by confirming that "the assurances explained in your letter…allow the European Union to deem…that DHS ensures an adequate level of data protection" (EU letter, 2007). On basis of the **DHS "assurances",** the new Agreement was signed on 23–26 July 2007, provisionally entering into force at the end of July.

The 2007 Agreement, with its threefold components (the Agreement, the DHS letter providing assurances about PNR privacy protection as practiced by the DHS and the EU's reply confirming that the level of protection was deemed adequate) is marked by two major tendencies. These are 1) the trend towards unilateral influence being exercised on the arrangements by the US side and 2) a considerable weakening of data protection safeguards (Article 29 Working Party, 2007, p. 2).

In view of the focus of this report on EU–Canada relations, the evaluation of the instrument is concise and confines itself mainly to highlighting the features that underline the current tendencies of a stricter, less privacy-minded treatment of passenger data.

As a general impression, it appears that the new instrument – as primarily shaped by the DHS assurances – tends to eliminate those interactive and negotiation-related elements that in the past led to lengthy bargaining between the parties. Above all, this applies to the **joint review mechanism**, which the US delegation had perceived as "extremely cumbersome".[165] From now on, the reviews will not take place annually but "periodically" and with the participation of only those officials or services deemed "mutually acceptable" (US DHS letter, 2007, Article X), thus excluding inter alia DPA expertise and oversight as one of the "main pillars of effective protection".[166]

Regarding the general level of data protection, the DHS assurances contain a somewhat enigmatic provision regarding reciprocity and the **mutual level of privacy protection** (s. IX). According to the Article 29 Working Party, the clause might be read in the sense that the future EU PNR system should not provide for a level of protection higher than that of the 2007 Agreement, which would be conceived as a "very worrying development" (Article 29 Working Party, 2007, s. 12).

In terms of individual privacy elements, the discussion follows the structure and terminology developed under section 3.2 above whereby only criteria of specific importance to the instrument in question are examined. Items 3.3 (Transparency) and 3.4 (Security) are thus omitted, as the 2007 Agreement does foresee any significant changes in their regard.

---

[165] Derived from oral evidence by Jonathan Faull, Director General for Justice, Freedom and Security (JLS), before the House of Lords EU Committee on 22 March 2007 (UK Parliament, House of Lords, 2007, p. 37).

[166] See Article 29 Working Party (2007), s. 10; see also European Parliament (2007), s. 9.

Item 3. Compliance with content principles

Item 3.1 Purpose limitation

From a procedural point of view, it is equally remarkable that, instead of negotiating amendments, the DHS will in the future just 'advise' the EU of any **changes affecting the agreed purposes** or other passages of the statement (US DHS Letter, 2007, s. I).

In "exceptional cases" or "emergency circumstances" (largely not further specified), the DHS reserves the right to unilaterally suspend certain provisions/safeguards concerning

- the transfer of PNR data to foreign governments without ensuring comparable data protection (ibid., s. II);
- access by the DHS to PNR data not found on the agreed list, including sensitive data (ibid., s. III); and
- denial or postponement of data access to data subjects as normally granted by the US Freedom of Information Act (ibid., s. IV).

And after all, it does not even seem clear whether the DHS assurances will be published in the US *Federal Register*, a condition for their becoming legally binding according to US law (Article 29 Working Party, 2007, s. 2).

Content-wise, it is criticised that – beyond the imprecise purpose descriptions found in the former agreement – the PNR may now expressly be used for **purposes far beyond serious criminality**, e.g. "for judicial purposes" in general, even in the case of petty crime or "as otherwise required by the law" (US DHS letter, 2007, s. I).

Item 3.2 Data quality and proportionality

List of data categories

Appearances may be deceiving: when the European Commission and the DHS proudly announced that the number of data elements listed had been reduced from 34 to 19, this seemed like good news. In reality, the new numbering was based on data groups (instead of individual elements). Moreover, since practically[167] all the elements from 2004 had been retained, partially by regrouping them with others,[168] and a few elements had even been added, the list had **increased from 34 to at least 37 elements** covered (Article 29 Working Party, 2007, s. 5).

Push method

Although the introduction of the push method had already been obligatory under the 2004 Agreement, the DHS continued to employ the **pull method** with direct access to airline computers at least in a number of cases. The 2007 DHS assurances mentioned 1 January 2008 as the ultimate date for completing the move, but doubts remain about this as a realistic assumption. Stumbling blocks could be that the DHS wants to have the final say on 1) the technical set-up of the push system, and 2) "when, how and what data to push" (US DHS letter, 2007, s. VIII). Furthermore, as the DHS wishes to obtain, in exceptional cases, additional data from the airline computers (ibid., s. III), observers wonder how this might technically work without employing the traditional pull method (Article 29 Working Party, 2007, ss. 5, 7).

---

[167] The only element deleted was "go show information".

[168] For example, the former items "12 Travel agency" and "13 Travel agent" became item "10 Travel agency/travel agent".

Retention period

The DHS assurances also introduced new retention periods, increasing the period from 3.5 to 7 years, and another period of 8 years was added during which the data is "dormant" (US DHS letter, 2007, s. VII). DPAs complain about this "highly worrying" result of **15 year's retention,** which is not compatible with recognised privacy standards (Article 29 Working Party, 2007, s. 9).

Item 3.5 Rights of access, rectification and opposition

The rights of data subjects remain vague, not least owing to the uncertainty about the legal character of the "assurances" and whether the latter confer formal rights or not (European Parliament, 2007, s. 6). As a positive step, the DHS extended administrative Privacy Act protection to non-US citizens and residents (US DHS letter, 2007, s. IV).

Item 3.6 Restrictions on onward transfers

Such transfers are **facilitated** by two changes: 1) the widened scope of acceptable purposes (see "Purpose limitation" above), which means that a considerable number of additional agencies may have a 'legitimate' interest in accessing PNR data, and 2) the abolition of the case-by-case requirement for such transfers. This might mean that PNR data could now be transferred in bulk format.

Fears voiced by critics regarding unilateral action by the US seemed to prove true in the **immediate follow-up** to the conclusion of the 2007 instrument: by letter of 30 July 2007, the DHS requested the EU to agree that all documents related to the negotiation of the Agreement "be held in confidence for at least ten years after entry into force of the agreement". In its reply to the DHS, the Council readily confirmed that the "EU shares your understanding regarding the **confidentiality of the negotiation process**" (Statewatch, 2007b, emphasis added).

And on 15 August 2007, the DHS announced a **change to US privacy provisions** having an important impact on the protection granted to airline passengers. The DHS as well as other agencies sharing its data were given exemptions from allowing access to data held on "entry processes", which includes PNR data (Statewatch, 2007a).

The evaluation of the 2006 interim instrument and the 2007 Agreement together with the surrounding negotiations definitely confirms the impression that at the least with the annulment of the 2004 Agreement in May 2006, the EU has lost considerable momentum in steering PNR discussions with the US. It seems as if a number of solid negotiation positions based on privacy protection and the rule of law were given up, without any serious attempt to oppose the often one-sided US requests. And the hope is deceptive that the needs/desires of the US will be satisfied once and for all – as the discussion under the following section shows.

3.3.4 A new generation of PNR commitments: Bilateral arrangements between the US and certain member states

Starting in early 2008, additional US security needs were invoked on yet another front, i.e. towards EU member states not yet part of the visa-free travel arrangements with the US. These included the new member states of the 2004 accession, mainly from Eastern Europe, as well as Greece.

In return for providing the US with concessions that were not covered by the EU–US Agreement, the member states were offered prospects of becoming part of the VWP. This involved the fulfilment of multiple conditions in terms of cooperation with the US, such as allowing armed sky marshals on board US-bound flights, the provision of PNR data beyond the

2007 requirements (e.g. regarding passengers not landing in but flying over the US and non-travellers – for example family members – who are allowed beyond departure barriers to help elderly, young or ill passengers to board aircraft flying to America). Furthermore, the countries concerned would have to accept the ETA system requiring all travellers to apply online for permission to travel to the US before they could buy a ticket (Traynor, 2008).

This move quite naturally conflicted with EU policy interests in both visa and PNR matters, which were based on a concept of a single negotiation approach with the US (see Box 6). All the warnings by the Commission that member states should avoid weakening the EU bargaining position were in vain, however: the Czech Republic acting as a forerunner ("Trojan horse")[169] signed the proposed MoU[170] on 26 February while others followed in the weeks after (Estonia, Latvia, Lithuania, Hungary, Malta and Slovakia).[171]

Box 6. The antecedents

The solo advance by the 2004 newcomers, although widely viewed as an act contrary to solidarity did not occur without reason, though. Since their accession, visa-free travel especially to the US had been among their primary policy goals; not only as a matter of prestige to be at the same level as the old member states but also because of the diaspora communities in the US.

Despite numerous complaints and despite the principle of solidarity prevailing in visa matters,[†] the EU institutions did not act energetically enough to defend the interests of the new member states. "There was no help, no solidarity from Brussels" (Traynor, 2008); instead, the newcomers were even "urged" not to lodge a formal notification in the sense of Regulation (EC) No. 851/2005, which would have triggered a reciprocity mechanism and ultimately led to the "temporary restoration of the visa requirement for the citizens of the third country concerned". In the case of the US, several of the old member states would not have been ready for such retaliation – "not least for fear of the massive disruption given the huge volume of transatlantic traffic" (ibid.).

[†] See Council of the European Union (2005), Regulation (EC) No. 851/2005.

In terms of a compromise, Brussels resolved the issue by letting the member states strike a deal with the US on 'minor' issues such as the sky marshals and national data exchange, whereas the Commission will remain in charge of the ETA issue (Goldirova, 2008).

Notwithstanding this temporary relief, prospects of a satisfactory solution remain modest and one might again think of a Pyrrhic victory for all the parties involved.

With the MoU signed, the new member states have entered into considerable obligations without obtaining a definite guarantee that they will soon benefit from visa-free travel. On the contrary, they will be exposed to practically permanent scrutiny by the DHS as to whether they fulfil expectations in "carrying out the security commitments" (Czech Republic–US, 2008, s. A.2), in question. And once designated as a VWP country, the member state would have to undergo periodic examination at least on a biannual basis in order to retain the status (s. A.2 of the MoU of 26 February 2008). In addition, what these countries might gain by fulfilling the conditions will not be the old style visa-free travel any more, but be subject to the ETA requirement that many consider just "a visa in disguise" (Goldirova, 2008).

[169] See Pospisil (2008).

[170] The complete text of the Czech Republic–US (2008) MoU is available online (retrieved from http://www.vlada.cz/scripts/detail.php?id=31921).

[171] See Goldirova (2008a).

For the EU, the situation implies a considerable loss of bargaining power in all related negotiations with the US; the possible 'coalition' between the US and individual member states in counteracting certain EU positions will always be pending as the sword of Damocles over forthcoming transatlantic talks such as the ETA/VWP issue and, of course, the PNR matters that are far from being resolved.

In view of the meagre results recently obtained and the visibly decreasing ability to achieve acknowledged privacy standards, in transatlantic negotiations one should dare to ask the basic question of what needs to be done in order to get back on track. Without going into the details, there is primarily one aspect that seems to have unbalanced the negotiation concept.

It is apparently not a problem of well-taken arguments: these have been sufficiently well presented with the help of the data protection authorities. If this reasoning – in contrast with the negotiations with Canada – did not manage to substantially influence the text finally agreed, this result had apparently to do with the entirely different importance attributed to privacy protection in the US, at least as long it may conflict with the interests of national security. And secondly, it appears that the US delegation is always able to put a much higher weight behind its bargaining position: such weight is not based on external elements of pressure but the attitude convincingly conveyed that they do **not need** the agreement.

This situation leads to the further question of why EU delegations constantly convey the opposite attitude, that Europe **could not live without** such an agreement – no matter how unfavourable the conditions under which it is concluded. This unbalanced scenario occurs not only in PNR negotiations but also in visa and other travel-related discussions. And it is quite likely to reappear in the forthcoming ETA negotiations. As a first consideration, one should enquire why – instead of suffering from endless concessions – Europe could not equally envisage a situation without an agreement. Or in visa waiver/ETA discussions, one might consider retaliating by similarly introducing a visa requirement for US citizens. Is it too daring an assumption to suppose that Americans would suffer as much from such a situation as Europeans?

In the end, one could expect that US delegations, when face to face with more determined European counterparts, would rather go for a reasonable compromise than extend the fighting forever.

A change of approach is urgently needed since the US seems quite decided to take the argument up to the next level by challenging the principle of data protection as such. According to the DHS Deputy Assistant Paul Rosenzweig, the "EU should reconsider its decision to apply notions of adequacy to the critical area of law enforcement and public safety. Otherwise the EU runs the very real risk of turning itself into a self-imposed island, isolated from the very allies it needs." This criticism is in first place addressed to the draft Framework Decision on data protection in police and criminal matters, since it "seeks to apply the same tired, failed standards of adequacy that it has applied in its commercial laws".[172]

4. Feasibility check: Do PNR instruments truly increase public security?

As we have seen in the previous sections, PNR data are but a small wheel in the overall machinery of border protection. By itself, PNR processing is worth nothing, as it is not even capable of achieving the most modest operational success; still, governments are ready to pay a

[172] See the statement reported in November 2007, *Statewatch News Online* (retrieved from http://www.statewatch.org/news/).

high price in terms of delicate intrusions into fundamental rights and possible international complications in order to take advantage of this 'small but precious pearl' for improving public security.

It is the intention of this short excursion into the field of border security to test the extent to which this precious element effectively adds to the overall efficiency of entry–exit systems or whether its deployment is compromised by other weak links in the chain.

Just for recollection, aside from making associations between known and unknown people, the main purpose of the PNR is to contribute to a more precise risk profiling and targeting of suspects;[173] according to the profiles, established border services can allocate their resources to specific hotspots on the border. Furthermore, the processing of PNR data is conceived to ensure seamless entry–exit controls through an improved coverage of all cross-border travel movements.

4.1 PNR and border-related securitisation: The direct impact

Evidence on direct hits achieved by PNR processing is extremely thin. It is understandable that governments, when asked to provide evidence on the value of PNR collection, are getting into difficulties. This has first to do with the ancillary character of this kind of data but also with the secrecy involved in the matching, targeting and other operations performed behind the scenes. The EU Committee of the UK House of Lords, when conducting a hearing on "The positive value of PNR" in March 2007, obtained several statements in that regard (see Box 7).

While expressing full understanding for the secrecy surrounding the highly sensitive area of national security, the House of Lords nevertheless regretted that it had to base its assessment more or less on hearsay evidence. Testimonies could have been given at least in a closed session, as it is an "important principle of democratic accountability that Parliament should be able to reach its own conclusions, and not have to rely on statements from the executive. This would help to secure public confidence" (UK Parliament, House of Lords, 2007, s. 22).

Box 7. Statements made to the UK Parliament House of Lords

According to Baroness Ashton of Upholland of the UK Department for Constitutional Affairs, there were a number of valuable examples of the benefits of PNR profiling in the areas of human trafficking and drug-smuggling operations, but no case could be cited regarding the fight against terrorism.

Jonathan Faull of the European Commission (DG Justice, Liberty, Security) mentioned several cases regarding terrorism and serious crime reported to him by the American partners, although sometimes only in outline, which proved the benefits of the PNR. But these findings were "very highly confidential" and could thus not be described in detail.

Similarly, Michael Chertoff, US Secretary of Homeland Security, when addressing various EU institutions in April and May 2007 made public, although "on an anonymous basis", some of the security achievements that resulted from data collected from the PNR, while giving examples of how the analysis of PNR data had prevented dangerous individuals from entering the US. Yet only one of the eight cases cited concerned the prevention of terrorism.

Source: UK Parliament, House of Lords (2007), ss. 19–21.

[173] See EDPS (2008).

4.2 What can go wrong: Collateral damages caused by data processing

Although assuming that in the absence of evidence to the contrary, one should accept that PNR data constitute a valuable weapon in the fight against terrorism and serious crime, the EU Committee also examined cases that had gone wrong. Alongside the widely known example of Senator Edward Kennedy being stopped several times at US airports because of a mismatch with an entry on a no-fly list,[174] there has been the tragic example of Maher Arar, a Canadian citizen of Syrian origin who spent almost a year in a Syrian prison cell owing to false conclusions drawn from correct PNR data by US and Canadian enforcement authorities.[175]

Such regrettable errors in terms of 'false positives' may arise from the bad quality of the original PNR record (e.g. misspelled names), but more frequently from careless management of watch lists or no-fly lists against which PNR data are matched.[176] The same applies to situations in which too many authorities are involved in the use/processing of the data or where system changes occur rather frequently.

With regard to our Canada-related topic, it should be noted that errors of the above kind are far more frequent under the US system with its swift sequence of newly tested screening or targeting devices, growing number of watch lists as well as rapidly rising number of agencies with access to the data in question. The more conservative Canadian approach with its a single data system (PAXIS) and less frequent changes in technical and policy matters appears less vulnerable to such incidents.

4.3 PNR and the concepts of seamless border protection

In its early days, API/PNR processing had been conceived as a method to ensure a seamless control of entry–exit movements, in particular in view of detecting visa over-stayers. Since then, the concept of complete control has not just survived the 9/11 events, it has gained additional momentum from the new counter-terrorist purposes under which the knowledge of 'who's in and who's out' has attained a still greater importance. Accordingly, the enormous efforts undertaken in improving API/PNR mechanisms are often seen in the context of completing a gigantic entry–exit system that will allow the tracing of movements and facilitate the pinpointing of suspects for easier apprehension.

Yet, this vision seems to suffer from a series of technical/organisational difficulties that reduce DHS officials to sheer despair. This concerns notably the US-VISIT system with its mission of faultlessly recording entry and exit movements with the help of biometric data. While control systems at airports (thanks to partially automatic/self-service devices) have come close to perfection, the long land borders with Mexico and Canada remain the Achilles' heel of the over-ambitious project.

Not much has changed since the conclusion drawn by the 9/11 Commission that "more than a half million persons enter the US illegally across the many thousand miles of land border every year".[177] Attempts to secure the Mexican border by means of fences, including 'virtual' ones based on watchtowers, electronic detection devices and cameras, have not achieved the results

---

[174] See the article by S.K. Goo, "Sen. Kennedy Flagged by No-Fly List", in the *Washington Post*, 20 August 2007.

[175] For a detailed description of the case, see subsection 1.1.2.1 of this report.

[176] See Nakashima (2007); see also Article 29 Working Party (2004a), p. 13.

[177] Derived from the UK Parliament, House of Lords (2007), s. 106.

expected.[178] Also, the lakes and rivers between Canada and the US offer ideal opportunities for illicit crossings, especially if one mixes on a sunny day with Michigan's thousands of recreational boaters on the Detroit River (Koslowski, 2005, p. 23).

But loopholes are not only found on the **'green' and 'blue' stretches of the border**, the heavily guarded and equipped **ports of entry** also prove vulnerable for various reasons (Koslowski, 2005, p. 28):

1) The immense **volume of approximately 330 million visa- and US-VISIT-exempt travellers per year** (US and Canadian citizens, as well as Mexican citizens with border-crossing cards) presents a perfect environment for unwanted foreigners (terrorist or others) to enter the US unrecognised and via official ports of entry.

2) The equally enormous **volume of daily commuters of up to 150,000 entries and exits per day** (San Ysidro/California–Mexico as well as Ambassador Bridge/Michigan–Canada) impedes control measures of beyond 10-15 seconds per car in order to avoid a complete shutdown of the port.

3) The **incapacity of technical devices**, including those working on the basis of radio technology or biometrics to ensure identity verification of every passenger is another weakness. There are easy ways to 'fool' radio-frequency identification border systems[179] as well as digital fingerprint devices (e.g. through 'fake fingers').[180]

The overall construction of such an integrated entry–exit system is extremely complex; beyond advanced technology, it also involves significant investment in the physical border infrastructure. Experts emphasise that the drive for 100% completion of the system and associated decisions are finally yet importantly budgetary ones. Are the president and Congress willing to expend sufficient financial and political capital to overcome these barriers? (See Koslowski, 2005, p. 63.)

These lessons should be kept in mind wherever else, Canada as well as the EU, the introduction of integrated border systems is being considered, whereby such advice applies to the overall system as well as individual components, including – as in our case – the highly sophisticated exploitation of passenger data. What is the benefit of investing dearly in a specific link of the chain if other parts will not fulfil the expectations?

Conclusions

As we have seen, the PNR is no more than a little though precious pearl among many on that long chain of elements called public security – even when looking at it solely through the narrow viewpoint of air traffic. It is more discrete than its straightforward colleagues such as API, which, thanks to its biographic data, can lead to direct hits and immediate implementation of no-fly orders. PNR operates more covertly and it requires permanent exchange/matching with other sources to produce significant results – a feature that represents at the same time its strength and its vulnerability.

---

[178] See the article "$20M 'fence' scrapped for not catching enough illegals", *CNN International*, 23 April 2008 (retrieved from http://www.printthis.clickability.com/pt/cpt?action=cpt&title).

[179] Under the NEXUS and SENTRI programmes, the enrolee receives a radio frequency (RF)-enabled proximity card. The RF-enabled chip on this card is read at the port of entry. It automatically pulls up background information and a photo for an inspector. The inspector can then quickly verify the NEXUS cardholder's identity and wave him or her through (Koslowski, 2005, p. 17).

[180] Ibid., p. 42.

We have tried to present how, after almost 40 years of peaceful existence in civil aviation, the PNR was discovered for enforcement purposes and how this facilitation tool that was initially created to best accommodate the personal preferences of passengers eventually became a post-9/11 device to track inclinations towards terrorist behaviour. Such a change of remit has implied several risks: a close neighbourhood with watch lists, targeting engines and other hardcore investigation devices, routine contact with a multitude of unconfirmed data and not least the natural risk of becoming itself the target of intense scrutiny by privacy watchdogs. Instead of enhancing civil liberties such as free movement, the PNR itself has suddenly become a threat to fundamental rights in terms of the data mining, mass processing and other deep intrusions into privacy.

The PNR story has thereby not been an isolated event but one that fits perfectly with overall securitisation strategies (extra-territorial controls, biometric features, a comprehensive system of entry–exit controls, etc.) which, besides tightening border security at home, have set up an extended border in order to keep possible offenders at the greatest possible distance away from territorial doorsteps. While transatlantic partners act increasingly in unison in this regard, a historic perspective reveals the extra-territorial aspect – as well as other strategies of massive border defences – as a specifically North American concept appropriate for common law countries, which traditionally reject the option of ID card-based controls within the territory. Continental Europeans, with their refined system of ID cards, would actually have much less reason to revert to such cumbersome strategies. The story of governmental intrusion being also one of resistance, we have equally looked at those who defend the civil liberties in question, identifying a number of fora at the parliamentary and judicial levels but most of all the DPAs, which do not all agree with the overall approach taken in PNR matters.

When testing the EU–Canada Agreement and its **legal compliance** (acceptability) with accepted international standards of privacy protection such as the OECD guidelines and Art. 8 of the ECHR, it has emerged that this instrument justly deserves its reputation as an island of peace in troubled waters: aside from a few partial objections, the overall system has been extremely balanced and has granted citizens appropriate protection and means of redress in case of intrusion.

Such judgment is all the more remarkable as it contrasts strongly with corresponding agreements concluded with the US. The EU–Canada instrument has shown an extremely low divergence rate from international standards (1.5 out 21), while the 2004 US Agreement failed to meet these benchmarks in more than two-thirds of the categories, including vital issues such as purpose limitation, transparency, proportionality, the retention period and appropriate citizens' rights to access, rectification and redress. Instead of improving, this score even deteriorated for the subsequent Agreements of 2006 and 2007, mainly owing to US tendencies to further downplay the importance of privacy protection in favour of a still more determined fight/war against terrorism and related crime.

The more prudent PNR approach chosen by the EU–Canada Agreement is also backed by considerations of practicability/feasibility and cost efficiency. Given that the most perfected front door devices in terms of airport entry control do not provide complete protection as long as the back door along land and sea borders remains wide open, especially to those who tend to disguise their movements, there does not seem much sense in investing too much – either monetarily or policy-wise.

It is good to remember these considerations: owing to the sunset clauses that are typical of good privacy-related legislation, the EU–Canada Agreement is soon due for a complete overhaul. In view of the pro-security/contra-privacy tendencies currently visible even in Canada (e.g. the no-fly provisions under the Passenger Protect Programme) and the EU (the future entry–exit system) one may be in doubt as to whether the balanced approach will survive the review

foreseen for the second half of 2008. It would be a pity if the EU–Canada instrument, instead of being a model for PNR legislation to come, were sacrificed to short-sighted enforcement considerations.

Policy recommendations

Based on the findings presented in this report, the following policy recommendations are put forward:

- The exploitation of PNR data for counter-terrorism purposes represents a highly sensitive matter that should be regulated with utmost care by the legislator.
- Decision-makers should be conscious of the quality of privacy as a fundamental right, which cannot be restricted or sacrificed for reasons of mere administrative/enforcement convenience. Any restriction must be carefully weighed in accordance with international data protection standards.
- As PNR data unfolds its potential for operational success as well as momentous errors in the framework of mass data processing and in combination with other data systems, regulatory bodies should set clear limits regarding 1) onward transfers to other agencies and 2) use of that data for purposes other than counter-terrorism. Onward transfers to other countries should be made dependant on the existence of adequate privacy standards in the destination country (adequacy finding).
- Any review or further extension of the PNR system should be preceded by a thorough analysis of the benefits that the measures are allegedly expected to produce. The argument of an increase in border security in general should thus be met with specific scepticism: as long as countries do not sufficiently master the control/surveillance of their notoriously porous land and water borders, a unilateral increase of airport and air traffic security is unlikely to produce any relevant results.
- Countries should abstain from adequacy findings based on mere assurances by PNR beneficiary countries. They should be ready to suspend further PNR transfers when there are reasonable doubts concerning the adequacy of protection.
- The 2006 EU–Canada Agreement represents an instrument beyond (almost) all criticism; forthcoming review talks should definitely seek to extend the validity of its existing provisions rather than aligning them with the doubtful standards of other recent instruments.

List of Abbreviations

API	Advance passenger information
APIS	Advance passenger information system
APP	Advance passenger processing
Article 29 Working Party	Data Protection Working Party under Art. 29 of Directive 95/46/EC
ATS	Automated Targeting System (US)
ATSC	Air travellers security charge (Canada)
CAPPS	Computer-Assisted Passenger Prescreening System (US)
CBC	Canadian Broadcasting Corporation
CBP	Customs and Border Protection (US)
CBSA	Canada Border Services Agency
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CLASS	Consular Lookout and Support System (US)
CRS	Computer reservation system
CSI	Container Security Initiative
DHS	Department of Homeland Security (US)
DPAs	Data protection authorities
ECJ	European Court of Justice
ECHR	European Convention on Human Rights and Fundamental Freedoms
EDPS	European Data Protection Supervisor
EPIC	Electronic Privacy Information Centre
ETA	Electronic travel authorisation
EURODAC	System for the comparison of fingerprints of asylum applicants (EU)
FAITC	Foreign Affairs and International Trade Canada
GDSs	Global distribution systems
IATA	International Air Transport Association
IBIS	Interagency Border Inspection System (US)
ICAO	International Civil Aviation Organisation
IDENT	Automated Biometric Identification System (US)
IRPA	Immigration and Refugee Protection Act (Canada)
IRRI	International Refugee Rights Initiative
ISE	Information sharing environment
MoU	Memorandum of understanding
NCIC	National Crime Information Center (US)
NGOs	Non-governmental organisations
OECD	Organisation for Economic Cooperation and Development
OPC	Office of the Privacy Commissioner of Canada

OSI	Other service information
PAXIS	Passenger Information System (Canada)
PIPEDA	Personal Information Protection and Electronic Documents Act (2000) (Canada)
PNR	Passenger name record
RFID	Radio frequency identification
SABRE	Semi-Automatic Business Research Environment
SIS	Schengen Information System (EU)
SSR	Special service request
TSA	Transportation Security Administration (US)
VIS	Visa Information System (EU)
VWP	Visa Waiver Program (US)
WMDs	Weapons of mass destruction

Bibliography

"28th International Conference of Data Protection and Privacy Commissioners" (2006), "Closing Communiqué", London 2–3 November (retrieved from http://ico.crl.uk.com/files/FinalConf.pdf).).

American Civil Liberties Union (ACLU) (2007), EU–US PNR agreement in light of 'Automated Targeting System', Letter to the European Parliament of 9 January, ACLU, New York (retrieved from http://www.privacyinternational.org/issues/policylaundering/ats/cavada.pdf).

Anti-Defamation League (ADL) (2004), *Canada and terrorism*, ADL, New York (retrieved from http://www.adl.org/Terror/tu/tu_0401_canada.asp).

Article 29 Working Party (1998), *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Working Document adopted by the Working Party on 24 July, Brussels (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf).

———— (2004), Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines, WP 88, 11 February, Brussels (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp88_en.pdf).

———— (2004a), Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), WP 87, 29 January, Brussels (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf).

———— (2005), Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, WP 103, 19 January, Brussels (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm#wp103).

———— (2007), Opinion 5/2007 on the follow-up 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 concluded in July 2007, WP 138, 17 August, Brussels (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf).

Australian Government (2008), "Fact Sheet 55 – The Electronic Travel Authority", Australian Department of Immigration and Citizenship, updated 28 March (retrieved from: http://www.immi.gov.au/media/fact-sheets/55eta.htm).

Bigo, D. (2006), "At the limits of the liberal state: The answers to the terrorist threat", *Re-public* (online journal), 16 November (retrieved from http://www.re-public.gr/en/?p=76).

Business Mobility Group (BMG) (2007), "Advance Passenger Information Systems", BMG (retrieved from http://www.businessmobility.org/API/API.htm.l#_Interactive).

Brimmer, E. (2006), "Safeguarding civil liberties in an era of security: A transatlantic challenge", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London/New York: Routledge, pp. 147–71.

Cameron, F. (2007), "Transatlantic Relations and Terrorism", in D. Spence (ed.), *The European Union and Terrorism*, London: John Harper, pp. 124–42.

Canadian Broadcasting Corporation (CBC) (2004), "Indepth: AIR CANADA – History", CBC, Toronto (retrieved from http://www.cbc.ca/news/background/aircanada/history.html).

Canada Border Services Agency (CBSA) (2003), Interim Memorandum D1-16-2, Interim Administrative Guidelines for the Provision to Others, Allowing Access to Others, and Use of Customs Information – Section 107 of the Customs Act, CBSA, Ottawa, 26 November ((retrieved from http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-2-i-eng.pdf).

————— (2005), "Advance Passenger Information/Passenger Name Record", CBSA, Ottawa (retrieved from http://www.cbsa-asfc.gc.ca/media/facts-faits/004-eng.html).

————— (2008), "Advance Passenger Information/Passenger Name Record", last updated on 16 January, CBSA, Ottawa (retrieved from http://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html).

————— (2008a), *Pre-Arrival Targeting Evaluation Study*, CBSA, Ottawa, January (retrieved from http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2008/target-ciblage-eng.html).

Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2007), "National ID Cards", CIPPIC, University of Ottawa, last updated 2 June (retrieved from http://www.cippic.ca/national-id-cards/).

Clarke, R. (2000), *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*, Australian National University, Canberra (retrieved from http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html).

Council of the European Union (2001), Regulation listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement of 15 March 2001 (EC) No. 539/2001, OJ L 81/1, 21.3.01.

————— (2002), Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002.

————— (2004), Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004.

————— (2004a), Decision 2004/634/EC concerning the conclusion of the Agreement between the European Community and the United States of America on intensifying and broadening the Agreement on customs cooperation and mutual assistance in customs matters to include cooperation on container security and related matters of 30 March 2004, OJ L 304/32 30.9.04 (retrieved from http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_304/l_30420040930en00320033.pdf).

————— (2005), Council Regulation amending Regulation (EC) No. 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement as regards the reciprocity mechanism, of 2 June 2005 (EC) No. 851/2005, OJ L 141/3, 4.6.2005.

Deutscher Bundestag (2007), Beschluß zum Bericht des Datenschutzbeauftragten, Drucksache 16/4882, Deutscher Bundestag, Berlin, 28 March (retrieved from http://dip.bundestag.de/btd/16/048/1604882.pdf).

Electronic Privacy Information Center (EPIC) (2006), *Privacy & Human Rights – An International Survey of Privacy Laws and Developments*, EPIC, Washington, D.C.

———— (2007), "EU–US Airline Passenger Data Disclosure", EPIC, Washington, D.C., last updated 13 November (retrieved from http://epic.org/privacy/intl/passenger_data.html).

———— (2007a), "Secure Flight", EPIC, Washington, D.C., last updated September (retrieved from http://epic.org/privacy/airtravel/secureflight.html).

———— (2007b), "Secure Flight Should Remain Grounded until Security and Privacy Problems are Resolved" EPIC, Washington, D.C., August (retrieved from http://epic.org/privacy/surveillance/spotlight/0807/default.html).

———— (2007c), "Automated Targeting System" EPIC, Washington, D.C., last updated 27 August (retrieved from http://epic.org/privacy/travel/ats/default.html).

ePractice.eu (2005), "EU gives green light to transfer of passenger data to Canada", *eGovernment News* of 19 July (retrieved from http://www.epractice.eu/document/873).

EurActiv (2007), "EU–US 'Open Skies' Agreement", Brussels, 9 October (retrieved from http://www.euractiv.com/en/transport/EU–US-open-skies-agreement/article-167482).

———— (2007a), "Central EU visa system will hold biometric data", EurActiv, Brussels, last updated 8 June (retrieved from http://www.euractiv.com/en/security/central-eu-visa-system-hold-biometric-data/article-133939).

———— (2007b), "Parliament slams PNR deal as 'substantively flawed'", EurActiv, Brussels, 13 July (retrieved from http://www.euractiv.com/en/justice/parliament-slams-pnr-deal-substantively-flawed/article-165524).

———— (2008), "Online privacy a concern for EU citizens", EurActiv, Brussels (retrieved from http://www.euractiv.com/en/infosociety/online-privacy-concern-eu-citizens/article-171742).

European Commission (2003), Communication on the Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, COM(2003) 826 final, European Commission, Brussels, 16 December (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0826:FIN:EN:PDF).

———— (2004), Annex, Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) (11 May 2004), Decision 2004/535/EC of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235, 06.07.2004, p. 11 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:EN:NOT).

———— (2005), *Joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004*, Commission Staff Working Paper, COM(2005) final, European Commission, Brussels, 12 December (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/review_2005.pdf).

———— (2005a), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, European Commission, Brussels, 24 November (retrieved from http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf).

———— (2005b), Decision 2006/253/EC of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the

Canada Border Services Agency, OJ L 91/45, 29.3.2006, p. 49 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:0060:EN:PDF).

———— (2006), *Report from the Commission to the Council and the European Parliament on transport security and its financing*, COM(2006) 431 final, European Commission, Brussels, 1 August (retrieved from http://ec.europa.eu/dgs/energy_transport/security/financing/doc/com_2006_0431_en.pdf).

———— (2007), "Passenger Name Record (PNR): Frequently Asked Questions", Rapid Press Release, MEMO/07/294, European Commission, Brussels, 13 June (retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/294&format=HTML&aged=0&language=EN).

———— (2007a), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, European Commission, Brussels, 6 November (retrieved from http://ec.europa.eu/commission_barroso/frattini/archive/COM(2007)654%20EN.pdf).

———— (2008), "EU–US Open Skies: A new era in transatlantic aviation starts on 30 March", Press Release, IP/08/474, European Commission, 28 March (retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/474&format=HTML&aged=0&language=EN&guiLanguage=en).

———— (2008a), Communication on preparing the next steps in border management in the European Union, COM(2008) 69 final, European Commission, Brussels, 13 February (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF).

———— (2008b), *Proposal for a Regulation of the European Parliament and of the Council…amending Regulation (EC) No. 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code*, COM(2008) 101 final, European Commission, Brussels, 22 February (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0101:FIN:EN:PDF).

European Data Protection Supervisor (EDPS) (2005), "Data protection as part of good governance in international organizations", Toolkit for workshop on 13 September, EDPS, Brussels (retrieved from http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/International_Org/Tool-kit_EN.pdf).

———— (2005a), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005) 200 final), OJ C 218/6, 6.9.2005 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:218:0006:0010:EN:PDF).

———— (2007), Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, EDPS, Brussels, 20 December.

———— (2008), Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, OJ C 110/1, 1.5.2008 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:110:0001:0015:EN:PDF).

European Digital Rights (EDRI) (2007), "Czech government accepts the new PNR Agreement with reservations", EDRI, 1 August (retrieved from http://www.edri.org/edrigram/number5.15/czech-pnr-reservations).

European Parliament (2005), "MEPs reject the EU–Canada agreement on transfer of personal data", Press Release, European Parliament, 7 July (retrieved from http://www.statewatch.org/news/2005/jul/ep-canada-pnr.pdf).

———— (2007), Resolution of 12 July 2007 on the PNR agreement with the United States of America, P6_TA(2007)0347, European Parliament (retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0347+0+DOC+XML+V0//EN).

European Parliament and Council of the European Union (1995), 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. OJ L 281, 23.11.95, p. 31 (retrieved from http://eur-lex.europa.eu/Notice.do?val=307229:cs&lang=en&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=&checktexte=checkbox&visu=#texte).

———— (2008), Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No. 2320/2002, OJ L 97/72, 9.4.2008 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:).

Foreign Affairs and International Trade Canada (FAITC) (2003), "Canada's Actions against Terrorism Since September 11", Backgrounder, FAITC, Ottawa, 7 February (retrieved from http://www.dfait-maeci.gc.ca/anti-terrorism/canadaactions-en.asp).

———— (2008), "Bilateral Air Negotiations between Canada and Foreign Countries", Canada and Foreign Countries Fast Facts, FAITC, Ottawa (retrieved from http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/facts-air-eclair.asp.x).

Frank, T. (2007), "6 states defy law requiring ID cards", *USA Today*, 18 June (retrieved from http://www.usatoday.com/news/nation/2007-06-18-id-cards_N.htm).

Geyer, F. (2007), *Fruit of the Poisonous Tree – Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy*, CEPS Working Document No. 263, CEPS, Brussels, September (retrieved from http://shop.ceps.eu/BookDetail.php?itemid=1487).

———— (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS CHALLENGE Paper No. 9, CEPS, Brussels, May (retrieved from http://shop.ceps.eu/BookDetail.php?item_id=1650).

Goldirova, R. (2008), "EU unity at stake over US visa regime Brussels warns", *EU Observer*, 11 March (retrieved from http://euobserver.com/9/25809).

———— (2008a), "Europeans to face tighter travel rules", *EU Observer*, 3 June (retrieved from http://euobserver.com/24/26260).

Goo, S.K. (2004), "Sen. Kennedy Flagged by No-Fly List", *Washington Post*, 20 August (retrieved from http://www.washingtonpost.com/ac2/wp-dyn/A17073-2004Aug19).

Grabitz-Hilf (2007), Das Recht der Europäischen Union. Bd. III Europäisches Datenschutzrecht. Loseblattsammlung, München: Beck, last updated October.

Greenemeier, L. (2004), "CAPPS II Is Dead, Says Ridge, But Door Is Open For CAPPS III", *Information Week*, 15 July (retrieved from http://www.informationweek.com/shared/printableArticle.jhtml?articleID=23901115).

Grossman, D. (2007) "An Airline Industry Wishlist", *USA Today*, 11 June (retrieved from http://www.usatoday.com/travel/columnist/grossman/2007-06-11-airline-challenges_N.htm).

Guild, E. (2007), "Inquiry into the EU–US Passenger Name Record Agreement", CEPS Policy Brief No. 125, CEPS, Brussels 22 March (retrieved from http://shop.ceps.eu/BookDetail.php?item_id=1481).

Guild, E. and E. Brouwer (2006), "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US", CEPS Policy Brief No. 109, CEPS, Brussels, 26 July (retrieved from http://shop.ceps.eu/BookDetail.php?item_id=1363).

Guild, E., S. Carrera and F. Geyer (2008), "The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?", CEPS Policy Brief No. 154, CEPS, Brussels, March (retrieved from http://shop.ceps.eu/BookDetail.php?item_id=1622).

Hamilton, S. (2006), "Transatlantic societal security: A new paradigm for a new era", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London/New York: Routledge, pp. 172–96.

Hasbrouck, E. (2007), "What's in a Passenger Name Record (PNR)?", Author's website article (retrieved from http://hasbrouck.org/articles/PNR.html).

Helmut, D. (2005), "The desert front – EU refugee camps in North Africa?", *Statewatch News Online*, March (retrieved from http://www.statewatch.org/news/2005/mar/12eu-refugee-camps.htm).

Hobbing, P. (2007), "A comparison of the now agreed VIS package and the US-VISIT system", Briefing Paper for the European Parliament, 4 July (retrieved from http://www.europarl.europa.eu/activities/committees/studies/download.do?file=17239).

International Air Transport Association (IATA) (2007), "IATA history", IATA, Montreal and Geneva (retrieved from http://www.iata.org/about/history).

International Civil Aviation Organisation (ICAO) (1970), "World Air Traffic Growth Rate Slackens in 1970", News Release, ICAO, Montreal, 31 December (retrieved from http://www.icao.int/icao/en/nr/1970/pio197017_e.pdf).

———— (2003), *The Canadian Advance Passenger Information Program*, FAL/12-WP/38, ICAO, Montreal, 11 December (retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf).

———— (2004), *Airline reservation system and passenger name record (PNR) access by states*, FAL/12-WP/74, ICAO, Montreal, 15 March (retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf).

———— (2004a), *Advance Passenger Information (API) – A Statement of Principles*, FAL/12-WP/60, ICAO, Montreal, 10 March (retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060_en.pdf).

———— (2008), *Harmonisation of advance passenger information requirements*, FALP/5-WP/4, ICAO, Montreal, 14 February (retrieved from http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp04_en.pdf).

International Refugee Rights Initiative (IRRI) (2004), "Anywhere but Here: Refugee Processing Centres in Libya", *Refugee Rights News*, Vol. 1, No. 1, October (retrieved from http://www.refugee-rights.org/Newsletters/NorthAfrica/V1N1AnywhereButHere.htm).

Joffe, J. (2007), "Wir wollen nur fliegen", *Die Zeit*, No. 34, 16 August, p. 1

Kagan, R. (2003), *Of Paradise and Power: America and Europe in the New World Order*, New York: Knopf.

Koslowski, R. (2005), *Real challenges for virtual borders: The Implementation of US-VISIT*, Migration Policy Institute, Washington, D.C (retrieved from http://www.migrationpolicy.org/pubs/Koslowski_Report.pdf).

———— (2006), "Border and Transportation Security in the Transatlantic Relationship", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London/New York, pp. 89–105.

Kroeger, A. (2007), "Malta struggles with migrants", BBC News, 7 July (retrieved from http://news.bbc.co.uk/1/hi/world/europe/6283736.stm).

Lettice, J. (2008), "EU squeals over US pre-flight personal data grab: Invasive DHS system just like the one we're building, apparently", *Register*, 11 February (retrieved from http://www.theregister.co.uk/2008/02/11/eu_dhs_eta_spat/).

Ludford, S. (2007), "Defending data", *Parliament Magazine*, 4 June, p. 15

McClure, G. (2007), "How Safe are Our Ports?", *IEEE News*, September (retrieved from http://www.todaysengineer.org/2007/Sep/port-security.asp).

Mulder, R. (2005), "The Birth of Air Transport", Author's website article (retrieved from http://www.europeanairlines.no/Arcticles_BirthofAirTransport_101004.htm).

Munroe, S. (2008), "Travel Documents for Canadians Going to the U.S.", *About.com: Canadaonline*, 30 January 2008 (retrieved from http://canadaonline.about.com/od/travel/a/traveldocsus.htm?p=1).

Nakashima, E. (2007), "Terrorism Watch list is Faulted for Errors", *Washington Post*, 7 September, p. A12 (retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601386.html).

Organisation for Economic Cooperation and Development (OECD) (1980), "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD, Paris, 23 September (retrieved from http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html).

Office of the Privacy Commissioner of Canada (OPC) (2003), "Breakthrough for Privacy Rights", Press Release, OPC, Ottawa, 9 April (retrieved from http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp).

———— (2005), "Privacy Protection in a World of Transborder Data Flows", Paper submitted by Jennifer Stoddart to the Organisation for Economic Cooperation and Development, OPC, Ottawa, 3 October (retrieved from http://www.privcom.gc.ca/speech/2005/sp-d_051003_e.asp).

———— (2007), Declaration of Civil Society Organizations on the Role Data Protection and Privacy Commissioners, Montreal, 25 September (retrieved from http://www.privcom.gc.ca/information/conf2007/res_ngo_06_e.asp).

———— (2007a), Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials, Passenger Protect Program – Canada's Aviation No-fly List, OPC, Ottawa, 28 June (retrieved from http://www.privcom.gc.ca/nfl/res_20070628_e.asp).

———— (2008), Proposed Immediate Changes to the Privacy Act, Statement by Jennifer Stoddart, Privacy Commissioner of Canada, Appearance before the Standing Committee on Access to Information, Privacy and Ethics, OPC, Ottawa, 29 April (retrieved from http://www.privcom.gc.ca/parl/2008/parl_080429_01_e.pdf).

Privacy International (2006), "EU–US passenger data transfer deal annulled by European Court", Privacy International, London, 30 May (retrieved from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-537923).

———— (2007), "Travel Privacy", Privacy International, London, last updated 18 December (retrieved from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559086).

Pipes, D. (2002), "Europeans: From Venus?", *Washington Post*, 16 July (retrieved from http://www.atypon-link.com/WDG/doi/pdfplus/10.1515/zstw.2006.117.4.852).

Pospisil, F. (2008), "Czechs became Trojan horses for new US visa waiver programme", European Digital Rights, 18 March (retrieved from http://www.edri.org/book/print/1450).

Rees, W. (2006), *Transatlantic Counter-terrorism – The New Imperative*, London/New York: Routledge.

Rötzer, F. (2007), "Von der Fehlerverlässlichkeit von Antiterrorlisten", *Heise online*, 12 April (retrieved from http://www.heise.de/tp/r4/artikel/25/25058/1.html).

Shimanek, A. (2001), "Do You Want Milk with those Cookies? Complying with the Safe Harbor Privacy Principles", *Journal of Corporation Law*, Winter, pp. 456–77.

Siskin A. (2005), *Visa Waiver Program*, CRS Report for Congress, Congressional Research Service, Library of Congress, Washington, D.C., 19 April (retrieved from http://www.ilw.com/immigdaily/news/2005,1116-crs.pdf).

Spence, D. (2007), "International Terrorism – The Quest for a Coherent EU Response", in D. Spence (ed.), *The European Union and Terrorism*, London: John Harper, pp. 1–29.

Spiegel Online (2004), "BGH-Urteil setzt Regierung unter Druck", *Spiegel Online*, 4 March (retrieved from http://www.spiegel.de/panorama/0,1518,289065,00.html).

———— (2007), "Schäuble will Unschuldsvermutung im Anti-Terror-Kampf nicht gelten lassen", *Spiegel Online*, Politik, 18 April (retrieved from http://www.spiegel.de/politik/deutschland/0,1518,477913,00.html).

Statewatch News Online (2005), "US: Report on airline passenger screening", *Statewatch News Online*, April (retrieved from http://www.statewatch.org/news/2005/apr/07us-passenger-screening.htm).

———— (2007), "EU: European Commission to propose EU PNR travel surveillance system", *Statewatch News Online*, updated 15 July (retrieved from http://www.statewatch.org/news/2007/jul/03eu-pnr.htm).

———— (2007a), "EU–US PNR agreement US changes the privacy rules to exemption access to personal data", *Statewatch News Online*, September (retrieved from http://www.statewatch.org/news/2007/sep/04EU–USa-pnr-exemptions.htm).

———— (2007b), "US demands 10 year ban on access to PNR documents", *Statewatch News Online*, September (retrieved from http://www.statewatch.org/news/2007/sep/02EU–USa-pnr-secret.htm).

Sullivan, B. (2006), "'La difference' is stark in EU, U.S. privacy laws", *MSNBC* (online), last updated 19 October (retrieved from http://www.msnbc.msn.com/id/15221111/).

Treasury Board of Canada, Secretariat (TBCS) (2005), "DPR 2004–2005, Canada Border Services Agency, Section II – Analysis of Performance by Strategic Outcome", TBCS, Ottawa (retrieved from http://www.tbs-sct.gc.ca/rma/dpr1/04-05/BSA-ASF/BSA-ASFd4502_e.asp).

Transport Canada (2001), "Government of Canada Introduces Public Safety Net", Press Release H147/01, Transport Canada, Ottawa, 22 November (retrieved from http://www.tc.gc.ca/mediaroom/releases/nat/2001/01_h147e.htm).

———— (2007), "Canada begins negotiations with European Union on Blue Sky's first anniversary", Press Release No. H 225/07, Transport Canada, Ottawa, 27 November (retrieved from http://www.tc.gc.ca/mediaroom/releases/nat/2007/07-h225e.htm).

———— (2007a), "Passenger Protect Program", Transport Canada, Ottawa, last updated 16 October (retrieved from http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm).

Traynor, I. (2008), "Bush orders clampdown on flights to US", *Guardian*, 11 February (retrieved from http://www.guardian.co.uk/world/2008/feb/11/usa.theairlineindustry).

UK Parliament, House of Lords (2007), *The EU/US Passenger Name Record (PNR) Agreement. European Union – Twenty-First Report*, European Union Committee, London, 22 May (retrieved from http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldeucom/108/10802.htm).

US Centennial of Flight Commission (2003), "Commercial Flight in the 1930s" (retrieved from http://www.centennialofflight.gov/essay/Commercial_Aviation/passenger_xperience/Tran2.htm).

US Department of Homeland Security (DHS) (2006), "Fact Sheet: Secure Borders and Open Doors in the Information Age", DHS, Washington, D.C., last updated 17 January (retrieved from http://www.dhs.gov/xnews/releases/press_release_0838.shtm).

———— (2006a), "Fact Sheet: Security Improvements to Visa Waiver Program", DHS, Washington, D.C., last updated 30 November (retrieved from http://www.dhs.gov/xnews/releases/pr_1164919987951.shtm).

———— (2007), "US-VISIT: How it Works", DHS, Washington, D.C. (retrieved from http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm).

———— (2007a), "DHS Announces Predeparture Screening of International Passengers and First Step Toward Secure Flight", Press Release, DHS, Washington, D.C., 9 August (retrieved from http://www.dhs.gov/xnews/releases/pr_1186668114504.shtm).

US General Accounting Office (GAO) (2004), *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, Report to Congressional Committees, GAO-04-385, GAO, Washington, D.C., February (retrieved from http://www.gao.gov/new.items/d04385.pdf).

Winer, J. (2006), "Cops across borders: The evolution of transatlantic law enforcement and judicial cooperation", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London/New York: Routledge, pp. 106–23.

Appendix I. Legislation, agreements and case law

Canada

Aeronautics Act (R.S., 1985, c. A-2) (retrieved from http://laws.justice.gc.ca/en/showdoc/cs/A-2//20080407/en?command=home&caller=SI&search_type=all&shorttitle=Aeronautics%20Act&day=7&month=4&year=2008&search_domain=cs&showall=L&statuteyear=all&lengthannual=50&length=50).

Regulations made pursuant to section 4 of the Aeronautics Act (1969–70, c. 45) (retrieved from http://laws.justice.gc.ca/en/showdoc/cs/R-5.3//20080407/en?command=home&caller=SI&search_type=all&shorttitle=Aeronautics%20Act&day=7&month=4&year=2008&search_domain=cs&showall=L&statuteyear=all&lengthannual=50&length=50).

Customs Act (1985, c. 1, 2nd Supp.) (retrieved from http://laws.justice.gc.ca/en/showdoc/cs/C-52.6//20080407/en?command=home&caller=SI&search_type=all&shorttitle=Customs%20Act&day=7&month=4&year=2008&search_domain=cs&showall=L&statuteyear=all&lengthannual=50&length=50).

Passenger Information (Customs) Regulations (P.C. 2003-908, 12 June 2003) (retrieved from http://gazetteducanada.gc.ca/partII/2003/20030702/html/sor219-e.html).

Immigration and Refugee Protection Act (IRPA) (2001, c. 27) (retrieved from http://laws.justice.gc.ca/en/I-2.5/).

Privacy Act (1980–83, c. 111), An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves, 1 July 1980 (retrieved from http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp#001).

Personal Information Protection and Electronic Documents Act (PIPEDA) (2000, c. 5)(retrieved from http://laws.justice.gc.ca/en/P-8.6/text.html).

European Union

Charter of Fundamental Rights of the European Union (Brussels, 7 December 2000), OJ C 364/1, 18.12.2000 (retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf).

Council of the European Union (2004), Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32004L0082%3AEN%3AHTML).

European Court of Justice

Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union* [2006] ECR-I 4721 (Judgement of the Court (Grand Chamber) of 30 May 2006, OJ C 178/1, 29.7.2006 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF).

Agreements and related documents

EU–Canada (2005)

Agreement between the European Community and the Government of Canada (Luxembourg, 3 October 2005) on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82/15, 21.3.2006 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:082:0015:0019:EN:PDF).

Related documents

European Commission (2005b), Decision 2006/253/EC of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, OJ L 91/49, 29.3.2006 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:0060:EN:PDF).

Annex to Decision 2006/253/EC of 6 September 2005 (*supra*), Commitments by the Canada Border Service Agency in relation to the application of its PNR Program of 11 May 2004.

EU–US (2004)

Agreement between the European Community and the United States of America (Washington, D.C., 28 May 2004) 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, OJ L 183/84, 20.5.2004 (retrieved from http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf).

Related documents

European Commission (2004), Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235/11, 06/07/2004 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:EN:NOT).

Annex to Decision 2004/535/EC of 14 May 2004 (*supra*), Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of 11 May 2004.

EU–US (2006)

[Interim] Agreement between the European Union and the United States of America (Luxembourg and Washington, D.C., 16–19 October 2006) on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298/29, 27.10.2006 (retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf).

EU–US (2007)

Agreement between the European Union and the United States of America (Brussels and Washington, D.C., 23–26 July 2007) on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204/18, 4.8.2007 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:EN:HTML).

Related documents

'DHS Letter (2007)'

Letter from Michael Chertoff, Secretary of Homeland Security to Mr Luis Amado, President of the Council of the European Union (undated), OJ L 204/21, 4.8.2007 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:EN:HTML).

'EU Letter (2007)'

Letter from Luis Amado, President of the Council of the European Union, to Michael Chertoff, Secretary of Homeland Security (undated), OJ L 204/25, 4.8.2007 (retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:EN:HTML).

Czech Republic–US (2008)

Memorandum of Understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America (26 February 2008) regarding the United States visa waiver program and related enhanced security measures (retrieved from http://www.vlada.cz/scripts/detail.php?id=31921).

Appendix II. Comparative table on PNR data elements collected according to various international instruments

Table AII.1 PNR data collected

EU–Canada Agreement 2005	EU–US Agreement 2004	EU–US Agreement 2007
1. PNR record locator	1. PNR record locator code	1. PNR record locator code
2. Date of reservation	2. Date of reservation	2. Date of reservation/issue of ticket
3. Date(s) of intended travel	3. Date(s) of intended travel	3. Date(s) of intended travel
4. Name	4. Name	4. Name(s)
5. Other names on PNR	5. Other names on PNR	5. Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.)
6. All forms of payment information	6. Address	6. Other names on PNR, including number of travellers on PNR
7. Billing address	7. All forms of payment information	7. All available contact information (including originator information)
8. Contact telephone numbers	8. Billing address	8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. All travel itineraries for specific PNR	9. Contact telephone numbers	9. Travel itinerary for specific PNR
10. Frequent flyer information (limited to miles flown and address(es))	10. All travel itinerary for specific PNR	10. Travel agency/travel agent
11. Travel agency	11. Frequent flyer information (limited to miles flown and address(es))	11. Code share information
12. Travel agent	12. Travel agency	12. Split/divided information
13. Split/divided PNR information	13. Travel agent	13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing field information	14. Code share PNR information	14. Ticketing information, including ticket number, one-way tickets and automated ticket fare quote
15. Ticket number	15. Travel status of passenger	15. All baggage information

Table AII.1 cont.

16. Seat number	16. Split/Divided PNR information	16. Seat information, including seat number
17. Date of ticket issuance	17. E-mail address	17. General remarks including OSI, SSI and SSR information
18. No show history	18. Ticketing field information	18. Any collected APIS information
19. Bag tag numbers	19. General remarks	19. All historical changes to the PNR listed in numbers 1 to 18
20. Go show information	20. Ticket number	
21. Seat information	21. Seat number	
22. One-way tickets	22. Date of ticket issuance	
23. Any collected APIS information	23. No show history	
24. Standby	24. Bag tag numbers	
25. Order at check in	25. Go show information	
	26. OSI information	
	27. SSI/SSR information	
	28. Received from information	
	29. All historical changes to the PNR	
	30. Number of travellers on PNR	
	31. Seat information	
	32. One-way tickets	
	33. Any collected APIS information	
	34. Automated ticket fare quote fields	

Source: Author's compilation.

About CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, but its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- To carry out state-of-the-art policy research leading to solutions to the challenges facing Europe today.
- To achieve high standards of academic excellence and maintain unqualified independence.
- To provide a forum for discussion among all stakeholders in the European policy process.
- To build collaborative networks of researchers, policy-makers and business representatives across the whole of Europe.
- To disseminate our findings and views through a regular flow of publications and public events.

Assets

- Complete independence to set its own research priorities and freedom from any outside influence.
- Formation of nine different research networks, comprising research institutes from throughout Europe and beyond, to complement and consolidate CEPS research expertise and to greatly extend its outreach.
- An extensive membership base of some 120 Corporate Members and 130 Institutional Members, which provide expertise and practical experience and act as a sounding board for the utility and feasability of CEPS policy proposals.

Programme Structure

CEPS carries out its research via its own in-house research programmes and through collaborative research networks involving the active participation of other highly reputable institutes and specialists.

Research Programmes

Economic & Social Welfare Policies
Energy, Climate Change & Sustainable Development
EU Neighbourhood, Foreign & Security Policy
Financial Markets & Taxation
Justice & Home Affairs
Politics & European Institutions
Regulatory Affairs
Trade, Development & Agricultural Policy

Research Networks/Joint Initiatives

Changing Landscape of Security & Liberty (CHALLENGE)
European Capital Markets Institute (ECMI)
European Climate Platform (ECP)
European Credit Research Institute (ECRI)
European Network of Agricultural & Rural Policy Research Institutes (ENARPRI)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)
European Security Forum (ESF)

CEPS also organises a variety of activities and special events, involving its members and other stakeholders in the European policy debate, national and EU-level policy-makers, academics, corporate executives, NGOs and the media. CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

E-mail: info@ceps.be
Website: http://www.ceps.be
Bookshop: http://shop.ceps.be

CENTRE FOR EUROPEAN POLICY STUDIES

Place du Congrès 1 • B-1000 Brussels
Tel: 32(0)2.229.39.11 • Fax: 32(0)2.219.41.51