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

Peter Hobbing

Abstract

Enhancing border security in support of the global "war against terrorism" is very much en vogue these days, in particular as regards the control of air passengers. Seven years after 9/11, this trend is yet unbowed. 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 "PNR mainstream", as embodied by the EU - US branch of transatlantic relations with its four agreements rapidly succeeding between 2004 and 2008, reveals the opposite tendency away from data protection and towards an unconditional tightening of controls. The paper undertakes to closely examine the doubtful benefits of such approach by looking at the price to pay *inter alia* for "false positive" mismatches and other collateral damages, while in turn the actual achievement of a higher degree of public security remains very much in the dark, most of all due to the impossibility of reaching a 100% tightness of borders. As a result, no stringent reason emerges why one should take leave from 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)

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, bottled liquids. We have become used to stand in endless queues waiting for security checks before boarding a transatlantic plane – or just transiting at an intermediary stop under the constant threat to miss your connection.

While excessive queues and similar obstructions are felt as 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 liberty "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 authorizations schemes which are about to come in vogue these days. "Why announce travel intentions 72 hours in advance?" upset passengers start asking and keep wondering how the inflation of security measures relates to global mobility, "open skies" and other liberal concepts which 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, maybe it is a tribute 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.

However, data processing even where done for high-ranking security purposes is not a game without rules. It is subject to international standards as developed by OECD and transposed into national law by the various member countries. The present paper therefore undertakes to check to what extent the criteria in question have been respected by the legislators. While such scrutiny - in view of the interests at stake -may not require any special justification, the reader may well ask the question why we examine these vital issues just on the basis of the 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 United States 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 PNR relations present a highly valuable research topic providing clues to all the strategies and tools available in airline security. On the one hand, the current 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.

---

* Peter Hobbing is Associate Research Fellow at CEPS.

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

On the other hand, this 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. Main indicators are the recent EU border package of February 2008 with a number of discomforting features which seem to be taken right out of the US "tool box" in border security, and 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 offers the east European EU members to join the VWP at the price of abandoning established European 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 situation and stressing the possible dangers of trying to turn back the wheel of time.

The paper will proceed in three steps, i.e. (1) retrace the metamorphosis of PNR airline data from a commercial facilitation device to a widely recognised tool of counterterrorism, (2) analyse to what extent the current use of this tool is acceptable, especially in terms of privacy protection, and (3) determine the practical benefits obtained from its use.

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

Airline history is that of the fastest growing transport industry: from the first powered flight (Wright Brothers 1903) to the first commercial passenger flight it took just 11 years[2], 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 becoming a standard only at the wake of WW II in 1939[3].

> In Europe as well as North America, internal services expanded considerably in the interwar years: 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 industrialized countries without a national airline. It was only in 1937, that the newly founded Trans-Canada Air Lines 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 meager 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).

The real airline boom occurred worldwide after WW II, when traffic increased by double digit rates practically every year between 1945 and 1970, while the total of annual passengers skyrocketed from 9 million to 311 million (ICAO, 1970). After some slow-down in the 1970's due to the first oil crisis, 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 is also mirrored in the success of the transatlantic routes: rising steadily, the annual

---

[2] Cf. "Airline" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Airline

[3] Cf. "Transatlantic flight" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Transatlantic_flight

passenger volume between EU and US has reached 50 million in 2007, thus becoming the by far biggest international air transport market. And its size is expected to expand by another 50%, thanks to the recent EU-US "Open skies" agreement (EurActiv, 2007; EU Commission, 2008). Similar negotiations are under way, under the keyword of "Blue Skies", between 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 between airlines in organising networks and performing a correct repartition of air fares in case of multi-sector trips ("revenue allocation") relied on more or less "hand-knitted" formulas, by 1960 at the latest the air 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 which could easily be exchanged not only between airlines but also 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 which had been gathered on air 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 of terrorism databases will lead to reliable results.

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

Under passenger data aspects, airline history can be sub-divided in roughly three phases: (1) the pre-electronic "pioneer" age, (2) advanced technology for travel facilitation purposes, and (3) Post 9/11: double exploitation for travel and security purposes.

1.1.1 PNR as instrument of travel facilitation

In the "stone-ages" of flying, the greatest achievement in travel booking (and important advantage over the railways as main competitor) was seen in the fact that it could be done by phone 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].

In 1946, the era of automated booking started with the electromechanical "Reservisor" installed by American Airlines, while tests commissioned by Trans-Canada Airlines (TCA) 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 are able to conduct

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

[5] Cf. "Computer reservations systems" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Computer_reservations_system

[6] „Semi-Automatic Business Research Environment", ibid.

reservation storage and retrieval operations as well as transactions involving the services provided by various carriers[7].

> Besides CRS initially created and run by the airlines themselves, there are now large **Global Distribution Systems (GDS)** which 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). Currently exist the following four GDS: Amadeus, Galileo, Sabre and Worldspan, whereby Amadeus is the only Europe-based system, 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) 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) itinerary of at least one sector, which must be the same for all passengers listed, and (5) name of the person making the booking.

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

While the above-mentioned five PNR elements are considered the minimum, there is a considerable amount of other information mostly required by both 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 phone contact numbers at their home address and intended destination.
- Age details if it is relevant to the travel, eg, unaccompanied children or elderly passengers requiring assistance.
- Frequent flyer data.
- "Special Service Requests" (SSR) such as special meal requirements, seating preferences, and other similar requests.
- "Other special instructions" (OSI), comments which are passed on to ground-staff to enable them to assist the passenger[10]

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 rentals or other which want to process their transactions by means of the GDS it is no surprise that PNR also arouses

---

[7] ibid.

[8] ibid.

[9] Cf. "Passenger Name Record" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Passenger_Name_Record

[10] ibid., for further details see the sample PNRs from SABRE and Galileo GDS in Annex I

the interest of government agencies which look at flight operations from an entirely different angle.

1.1.2 Post-9/11 developments and its precedents

Koslowski 96f,

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 still nowadays they are 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 as such 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 obtain to achieve political and publicity goals such as 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 60s, Palestine-Israel, 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 move, the **in-flight destruction of aircraft** as well as the killing of the 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, there were numerous attacks of a similar kind before and after.[13]

The landmark events of the 9/11 suicide attacks were finally characterized by a further escalation: in addition to annihilating 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 pursuing a concrete political purpose.

Beyond the technique of the terror assault, 9/11 represented also **landmark in terms of responses to the threat of hijacking**: reactions resulted first of all in a number of technical measures to address the specific risks which 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; from now on the policy was to prevent access to the cockpit and pilots. At check-in, air passengers worldwide were prohibited from carrying anything remotely like a bladed weapon in the passenger cabin: scissors, tweezers, nailfiles, etc.[14]

On a more general level, the events revealed a long list of security vulnerabilities of global transportation and border control systems (Koslowski, 2006, p. 89), especially with regard to the supervision/enforcement of visa and passport requirements. According to these findings, "at

---

[11] Already during the early 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). Cf. "Surveillance aircraft" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Surveillance_aircraft

[12] for further examples see „List of aircraft hijackings" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/List_of_notable_aircraft_hijackings

[13] cf. „History of Terror Attacks" History Central. History's home on the web. Retrieved from http://www.multied.com/Terrorhistory.html

[14] cf. FAA 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 Commission list of 16.1.04 as amended on 5.10.06 to include explosive liquids, cf. Regulation (EC) No 2320/2002, OJ L 355, p.1

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 (BCBP), to manage the collection, transfer and retention of PNRs.

America was shocked after the events of 9/11, but it wanted to show that was able to "fight back", to react quickly and provide a reliable defence which rendered impossible similar incidents in the future[15]. What America sought 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 want to abstain from discussing too many details. What counts, however, is that 9/11 as well as the intended revolution had a direct impact [schwappte in andere Länder über] 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" (ATSA), which required all airlines with US-bound international flights to submit a passenger manifest electronically and 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 (#8) and the set-up of Joint Passenger Analysis Units (JPAU) (#9).

The internal Canadian requirement for airlines to provide API/PNR data had been adopted shortly before, by the new Public Safety Act of 22 November 2001[18]. Although there had 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-Canada relations. The same holds true for the Canada Anti-Terrorism Act adopted shortly after 9/11 as "mirror image" of the USA 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, ie the bombing of Air India flight 182 in June 1985 which until the 9/11 events was the single deadliest terrorist attack

---

[15] The DHS was assigned/expected to „manage who and what enters our homeland" [Koslowski, Fn 6]

[16] R. Falkenrath, Deputy Assistant to the President and Deputy HS adviser, as cited by Koslowski (2006), p. 92

[17] US code, Title 44909. Passenger manifests. http://www4.law.cornell.edu/uscode/49/44909.html

[18] cf. http://www.tc.gc.ca/mediaroom/releases/nat/2001/01_h147e.htm

[19] cf. „Canada's Anti-Terrorism Act". Maclean's Magazine of 25 October 2004. Retrieved from http://www.thecanadianencyclopedia.com/index.cfm?PgNm=TCE&Params=M1ARTM0012675

involving aircraft[20]. The attack which killed 329 persons en-route from Montreal to India was accredited 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 counterterrorist 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 US and Canadian enforcement authorities. When it eventually became clear that there was no valid evidence against him, the Canadian Government awarded Arar C$10.5m (Euro6.9m) in compensation, the highest settlement by the Canadian Government in an individual human rights case[21].

1.1.2.2 Transatlantic relations (EU - US, EU - Canada)

Post-9/11 solidarity prevailed also on the other side of the Atlantic: the EU Heads of State and Government met for an extra-ordinary European Council on 23 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, the Framework Decisions on terrorism, on the freezing of assets of those suspected as terrorists.

However, 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, US Customs[22] (and later the Canadian CBSA) since January 2003 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 allowed 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 EU Commission started negotiations with the CBP which eventually led to the conclusion of the 2004 EU-US agreement in PNR matters[23]. The agreement itself rests on two vital pillars, i.e. the EU adequacy finding that the data will be "adequately protected" in the US ("safe harbour" situation) and the corresponding "undertakings" by 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), 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 the previous US experience, the EU reacted swiftly and entered into negotiations which led to the EU – Canada Agreement in API/PNR matters of 3 October 2005.

However, as regards EU-US relations, the peace did not last long; following annulment by the European Parliament (EP), the European Court of Justice (ECJ) on 30 May 2006 annulled the

---

[20] see „Air India Flight 182", http://en.wikipedia.org/wiki/Air_India_Flight_182

[21] For a detailed description of the case, see HoL (2007), p.12

[22] 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 (cf. EPIC 2007).

[23] Agreement of 17.5.2004, OJ L 183/84 of 20.5.04

[24] for a detailed description of the PNR instruments see Sections 2.2., 2.3 below

[25] for details see Art. 29 WPDP

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. Also the new agreement signed in July 2007[27], with hardly any improvements in comparison to its predecessor, is far from pleasing all 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 which might weaken privacy provisions to a still greater extent[28].

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

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 to go for and, last but not least, 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 which 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 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; while the imposed access to PNR has frequently been characterized as a bold move by security agencies to “jump on the bandwagon”, API concerns data which 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 which 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 risk which airline associations see with some scepticism (ICAO 2008).

---

[26] cf. ECJ (2006); see part 3.3.2 below

[27] cf EU – US (2007); see part 3.3.3 below

[28] cf Czech Republic – US (2008); see part 3.3.4 below

[29] cf. Canadian Advance Passenger Information/Passenger Name Record (APS/PNR) program based on section 107.1 Customs Act, Passenger Information (Customs) Regulation, paragraph 148 (1)(d) of the Immigration and Refugee Protection Act and regulation 269 and of the Immigration and Refugee Protection Regulation.

[30] Cf. Lufthansa, API (Advance Passenger Information). Retrieved from http://www.lufthansa.com/online/portal/lh/cmn/generalinfo?l=en&nodeid=1795851&cid=

1.2.1 Data collection via PNR, 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 which can be directly taken from the machine-readable part of a passport plus the general flight-related data which are anyway in the airline computers, eg. as required under Directive 2004/82/EC (EU Council 2004)[31].

The list includes the following elements which are of an evident interest for investigators as they allow to directly establish the identity of a person:

- number and type of travel document used,
- nationality,
- full names,
- the date of birth,
- the border crossing point of entry into the territory of the Member States,
- 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 which will be much more difficult to handle and are therefore vehemently opposed by the associations (ICAO 2008).

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 ICAO standards, it is sufficient that PNR contain the following 5 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/GDS may contain the same data fields but the fields are listed under different names and in a different order. Sometimes fields are split up in two or

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

[32] to make the booking compliant with the IATA Reservations Services Manual (cf. ICAO 2004)

vice-versa several fields regrouped under one header 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 which governments want to collect from air industry. None of the lists attached to the 4 EU instruments so far existing/proposed in PNR-matters (EU-US agreement 2004, EU–Canada agreement 2006, EU–US agreement 2007, draft Framework Decision 2007) are alike.

> In some cases it is just a change of terminology, ie the same subject is bears another label, sometimes the order of subjects has been altered which adds to the confusion in view of the length of the list (up to 34 items) and most of all the tendency to present shorter lists without sacrificing any content. This is particularly true for the EU – US agreement 2007 which in an (alleged) effort to comply with privacy-related criticism shortened the list of items from 34 to 19 – however, only two data elements were effectively deleted, all the rest reappeared under another header (cf. the detailed comparison published by Statewatch 2007, p.6)

- **commercial orientation** of data collected

Many fields are of a more technical nature (eg. seat number, 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", labelled "special service requests" (SSR), "Other Service Information" (OSI) and "General remarks". It is here where one would find references to special dietary preferences, health needs or similar elements which in turn could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or characteristics concerning health or sex life of the passenger. On the other side, such sensitive data whenever found in these fields, should be seen as "off limits" for security staff (cf. EU Commission 2004 with regard to the 2004 EU-US agreement).

So all that PNR can possibly deliver has would require a painstaking screening of the technical data items in the hope to establish patterns and matches with specific crime/terrorism-related data collections. This aspect will be deepened under para 1.

1.2.2 Data transfer from air 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 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 (MRZ) of EU passports[33], 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) which will run checks against security and intelligence watch-lists connected to the system. Also known as "Board/No Board" and "Red Light/Green Light System", APP transmits the data to border control agencies prior to flight departure and receives in turn a

[33] It should be noted, though, that Canada requires airlines to transmit with API, certain data elements which 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 (cf Lufthansa notice http://www.lufthansa.com/online/portal/lh/cmn/generalinfo?l=en&nodeid=1795851&cid=)

directive for each passenger either permitting or denying boarding (ICAO 2004a)[34]. In the case of Canada, the API system is PAXIS whereby 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 due 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 first place neither from their technical architecture nor from the content stored and processed. Furthermore companies handling PNR at airline or distribution system (GDS) level have neither the skills nor the interest to perform 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 ("pull system") rather than sorting out the relevant data themselves and transmitting it to the authorities ("push system").[35]

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

The "pull"-system has in the meantime been recognized as being in clear violation of privacy rights as laid down, at the international level, by the OECD Guidelines of 1980[36] as well as 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 (cf. EDPS 2007a)[37]. It is not sufficient that the foreign security authority (in the case of EU-US relations, US Customs and Border Protection – CBP) commit themselves to delete the "surplus" data at a later stage. Appropriate protection of passenger interests requires that such data is filtered before and not after its transmission to a third country.

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

> It is stressed that the initial costs to support a pull system are relatively minor in comparison to 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 systems: For carriers operating a large number of flights in an affected market, this cost could run to "hundreds of thousands of dollars per year" (ibid).
>
> 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 which 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 government(s) requesting the data (ibid).

---

[34] US Customs and Border Protection call this process AQQ (Apis Quick Query) leading to a "cleared" or "not cleared" message being sent back for each passenger (Statewatch 2007).

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

[36] http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html

[37] 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 below.

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 carriers which continue using the "pull"-procedure may be exposed to possible liability claims filed by passengers concerned. After years of discussion[38], 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" (EU Commission 2008a: Article 5).

1.2.3 Exploitation of PNR data by security authorities

The exploitation of the passenger data obtained represents in a way the "ultimate leg" to come 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 which might make sense in combination with items found elsewhere, just like pieces of a big puzzle.

In the case of PNR, the situation is particularly obvious: none of the data retained in such records would on its own reveal a specific threat or even suspicion 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, PNR has no such straightforward content.

The more "discreet" significance of PNR holds true for simple items (seat number, date of reservation etc) just as much as for the more sensitive SSR or OSI fields which potentially reveal passenger preferences and other circumstances such as "won't fly on the Jewish sabbath", "uses wheelchair" (Hasbrouck 2007). 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 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 two-fold strategy, i.e. first of all it is about scoring a hit on the passenger in question while running his data against watch-lists and other data resources, and secondly to widen the scope of information available when this data is retained and stored for future checks.

Major systems used for routinely scrutinizing PNR data are the following:

1.2.3.1 United States

The US have certainly gathered the greatest amount of experience in the automated screening of airline passengers. Over the years various names have surfaced such as CAPPS (Computer Assisted Passenger Prescreening System), CAPPS II, ATS (Automated Targeting System) and

---

[38] Cf Commission report of 1 August 2006 concluding that the implementation of Community legislation on airport security is a task which 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" (EU Commission 2006, p. 5f)

..

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 have tested and employed various programs, we also know that some of them were abandoned (CAPPS I and II) due 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**

As all its successors, the original CAPPS, first implemented in the late 1990s[39], served to target potential terrorists by checking their PNR data against TSA terrorism watch-lists[40] whereby passengers selected for special checks (so-called "selectees"[41]) 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 the controls were not carried out[42].

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 now run by a government agency (TSA) instead of the commercial carriers in charge under CAPPS I. There was an expanded selection of PNR data which 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 General Accounting Office (GAO) stating that CAPPS II had not done its homework in 7 out of 8 areas for which improvements had been requested before (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. Passengers concerned had neither access to the data nor ways to challenge an unfavourable risk designation (Greenemeier 2004).

- **ATS**

While the public still speculated about the creation of a CAPPS III system, DHS-CBP had already extended its Automated Targeting System (ATS), originally conceived to "target oceangoing cargo containers for inspection", to include travellers. Its new function was discovered only by November 2006, when DHS published a "Notice of Privacy Act system of records"[43] requesting the exemption from crucial provisions of the Privacy Act of 1974 (EPIC

---

[39] 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 (cf. "Computer Assisted Passenger Prescreening System" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Computer_Assisted_Passenger_Prescreening_System

[40] PI (2007)

[41] found on the „selectee" list administered by the Transportation Security Administration (TSA) as opposed to the "no fly" equally managed by TSA, cf PI (2007)

[42] cf. Wikipedia ibid.

[43] DHS, Federal Register: November 2, 2006 (Volume 71, Number 212), retrieved from http://edocket.access.gpo.gov/2006/06-9026.htm

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 ATS even in the performance of its limited container-related tasks, giving it a low marks ("C-/D+") in a 2006 scrutiny report by the House Homeland Security committee and making 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 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 DHS in August 2007 (cancellation of exemptions from the Privacy Act, establishment of comprehensive passenger redress procedures under the DHS TRIP program)[44], the current operation of ATS and its relationship to its Secure Flight counterpart remain widely in the dark.

- **Secure flight**

Almost simultaneously to the ATE announcement, DHS presented its new Secure Flight program[45] to conduct uniform prescreening of passenger information against federal government watch lists for domestic and international flights. In its screening routine, SF intends to identify "suspicious indicators associated with travel behaviour" in passengers' itinerary PNR data (EPIC 2007a). Due to numerous security vulnerabilities detected by government reports as early as 2006 (PI 2007) including "significant weaknesses" of the terrorist watch-lists available[46], it seems that the official operation of the SF will remain grounded until 2010. Public trust in the watch-lists has also been undermined by news reports according to which airmarshals were subject to a "quota system in reporting terrorist profiles"[47].

Still one cannot be sure what is really going; reports are contradictory and it seems that, under the auspices of secrecy, government sources avoid to provide a comprehensive description on all ongoing activities in air passenger screening. Characteristically enough, none of the reports dealing with 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 Canada Border Services Agency (CBSA): there is just one agency in charge (CBSA), one program to check PNR and API (PAXIS) and a concise and understandable description accessible to all those interested in the matter.

- **PAXIS** (Passenger Information System of the Customs and Border Service)

---

[44] DHS, Federal Register: August 6, 2007 (Volume 72, Number 150) retrieved from http://edocket.access.gpo.gov/2007/E7-15198.htm

[45] cf. DHS Press release of 9 August 2007, http://www.dhs.gov/xnews/releases/pr_1186668114504.shtm

[46] cf. "Terrorism Watch List is Faulted for Errors", Washington Post of 7 September 2007, p. A12. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601386.html

[47] For promotion purposes „Each federal air marshal is now expected to generate at least one SDR [Surveillance Detection Report on air passengers] per month." http://www.thedenverchannel.com/news/9559707/detail.html

The PAXIS system created in 2002 in the follow-up to the Canadian Antiterrorism Act of 18 December 2001[48] serves to provide automated risk assessment of pre-arrival data transmitted by air carriers to the CBSA via Electronic Data Interchange, e-mail and the Internet (TBCS 2005).

In contrast to corresponding US systems, PAXIS deals with API and PNR in absolutely the same manner: not even API data needs to be transmitted before departure of the plane, it is sufficient, if transfer takes place within 15 minutes before landing in Canada. This implies that Canada – at least in so far – does not employ the "no fly" option, i.e. to interdict, in case of high risk travellers, the boarding of the aircraft at the airport of origin. All that PAXIS does in this context is a pre-arrival targeting of travellers in the sense that it recommends certain persons to 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 out 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 embarassing errors which seem so significant for fully automated lists e.g. in the US.

Similar to the EU-Canada Agreement, the PAXIS risk assessment and targeting system has evoked very little concern neither among passengers nor with privacy authorities or NGOs. The most important factors for this positive appreciation may be the following

- absence of fully automated mechanisms such as "no fly" orders in combination with unreliable watch-lists
- common sense adjustment of automated PAXIS risk score by NRAC targeting specialists
- full transparency of screening/targeting procedures employed
- access to redress procedures for passengers affected[49]
- 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 neither by passengers nor by government commissions which would see a need for radical reforms.[50]

This being said, one needs to look also at another, more recent aspect of Canadian threat prevention which clearly obtains much less applause.

- **Passenger Protect Program (**Passenger Information System of the Customs and Border Service)[51]

Since 18 June 2007, Canada operates the Passenger Protect Program with a "No fly"-mechanism as its centre piece, very much in line with the before-mentioned US examples. The

---

[48] Bill C-36 http://www2.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Parl=37&Ses=1&Mode=1&Pub=Bill&Doc=C-36_4

[49] cf. Interim Administrative Guidelines for the Provision to others, Allowing access to others, and Use of Customs Information**,** http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-2-i-eng.pdf

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

[51] for a program description, see Transport Canada (2007a)

new rules, adopted as government regulations (no involvement of parliament!) under the Aeronautics Act[52] and the authority of the Minister of Transport, foresee the establishment of a "No-fly" list, comprising individuals

(a) involved/suspected to be 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

(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 composed 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 that 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 hours duty service will in turn take an immediate decision to issue or not 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):

- lack of a legal basis in the Aeronautics Act for adopting such program,
- lack of adequate protection, under the current Privacy Act, against the privacy risks resulting from such initiative
- no safeguard available 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 legally enforceable right of appeal for the traveller.
- 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"[53]. 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 side, 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 the European point of view, it is not apparent to which extent international flights are/will be affected by the programme: at least flights from/to EU destinations seem to be exempt. As laid down above, the EU-Canada agreement in API/PNR matters is very clear about API/PNR data: they do not have to be transmitted before departure and will be used for the purpose of a secondary screening only, which logically excludes any "no-fly" option.

---

[52] based on sections 4.76, 4.77 and 4.81 of the Aeronautics Act of 1985, http://laws.justice.gc.ca/en/ShowFullDoc/cs/a-2///en

[53] C. Baggaley, Strategic Privacy Advisor at OPC in his letter to the author of 5 May 2008. He stressed, however, that "very few, if any, passengers have been denied boarding".

1.2.4 Results expected and obtained

Despite the full trust and high expectations 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 motivated by 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 in PNR-matters. The EU Commission report on this event complained about the "limitations imposed on the number of records that could be accessed and on the provision of hard copy versions of certain staff procedural guidance." (EU Commission 2005, p. 6)[54]. Equally Canada's Privacy Commissioner, Jennifer Stoddard, was disappointed to hear that the new watchlist/"no-fly" program was based on "practical global experience and risk assessment rather than specific studies."

It can be hoped that the forthcoming review on 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 environment represents the biggest challenge for airlines[55]: according to 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[56].

It seems accepted in general that security costs be shared among the various parties concerned, ie they "should be borne by the State, the airport entities, air carriers, other responsible agencies, or users" (Art. 5 Regulation (EC) No 300/2008[57]), whereby there is disagreement as to the respective size of these shares. The EU exceptionally allows state aids in so far as they are directly linked to security purposes (ibid).

As regards the airlines, the subject of PNR costs seems not a subject of primary dissatisfaction any more; 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 item does not show

---

[54] Cf. also European Parliament resolution P6_TA-PROV(2007)0347 of 12 July 2007 on the PNR agreement with the United States of America, http://www.statewatch.org/news/2007/jul/ep-pnr-resolution-jul-07.pdf

[55] IATA Director General Giovanni Bisignani, USAtoday of 11/06/2007. http://www.usatoday.com/travel/columnist/grossman/2007-06-11-airline-challenges_N.htm

[56] in Canada for domestic itineraries, the Air Travellers Security Charge (ATSC) is currently 5 CAD one-way to a maximum charge of 10 CAD. For transborder itineraries, the ATSC is 8 CAD / 7 USD one-way to a maximum charge of 16 CAD / 14 USD, cf. http://www.aircanada.com/shared/en/common/flights/pop_surcharge.html

Regular complaints are heard also in Europe, eg. 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", http://news.bbc.co.uk/2/hi/uk_news/7025419.stm

[57] Cf EU Commission (2008a)

up any more in recent publications – possibly due to established cost-cutting routines. The EU Commission currently estimates PNR costs at 0.20 Euro per passenger[58].

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

2. PNR and the wider security landscape

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

2.1 Visions of a perfect border: seamless protection and extraterritorial action

This interdependence is all the more crucial when looking at security in a wider context: "total security" as it is increasingly strived for on both sides of the Atlantic requires 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 increasingly challenged by complying with the contradictory targets of a maximum of mobility on the one and a maximum of security on the other side.

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 sort of a miracle solution, the IT approach promises to transform border lines in unsurmountable obstacles towards 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 streamlining approach to avoid the system to be 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.

This being said, one should not conceal, that the "perfect border" as envisaged is costly in various respects, ie financial and human resources as well as sacrifices in terms of civil liberties. And beyond all this, there are considerable doubts to what extent 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 "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.[59]

---

[58] Information provided by DG JLS on 10 April 2008

[59] for further details see Section 4.3 below

The following remarks intend to outline major solutions proposed under the auspices of both "tight and streamlined borders" and "extraterritorial 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 they introduced **US-VISIT**, the first "automated entry-exit system", originally conceived for immigration purposes to detect visa overstayers (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 traveller is again checked by means of comparison with the data stored in IDENT.[60] The US-VISIT/IDENT system provides, by the way, for a far-reaching interoperability with the databases operated under the aegis of DHS. Biometric exit controls are facilitated by automated, self-service kiosks which are integrated in the airline check-in procedures.

> The system is insofar air-tight as it includes – in principle – all travellers, no matter whether subject to visa obligation or not: the former privilege of the so-called visa-waiver countries[61] was abandoned in 2004[62]. The only remaining exemptions from US-VISIT are valid for Canadian citizens in general and certain groups of Mexicans.
>
> The US employ currently no "bona fide traveller" programme to expedite the entry/exit control for foreigners; it is only at US consulates abroad where "bona fide"-applicants may find simplified procedures when applying for a visa (DHS 2006).

Within the **EU[63],** there is up to now just a fragmentary coverage of entry-exit movements: 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 to check their identities 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 finger prints) to identify persons who have lodged a visa application for 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 SIS II and VIS even

---

[60] for details see Hobbing (2007)

[61] including the following EU Member States: Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Luxembourg, Netherlands, Portugal, Spain, Slovenia, Sweden and UK. The only privilege which remains VWP countries is that their citizens do not have to undergo the costly and time-consuming visa application procedures at an US consulate back home.

[62] After the attempt of a UK citizen (Richard Reid) to detonate a bomb hidden in his shoe in a transatlantic flight, it was considered to abandon the VWP altogether. Instead the US Congress decided to keep the VWP but subject its beneficiaries to the requirements of the US-VISIT program (cf. Koslowski 2005).

[63] For a detailed description

[64] Cf. EU 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; cf. http://europa.eu/scadplus/leg/en/lvb/l33081.htm

share a common technical platform, there is so far no interoperability between them or with EURODAC (Hobbing 2007)[66].

In early 2008, the EU Commission decided to reconsider the situation by presenting its vision of a future European **entry-exit system** (EU Commission 2008b). Under the motto "The next steps", it is proposed to introduce a full-fledged entry-exit system based on (a) the **registration,** in an entry-exit database, of all third country nationals entering EU territory[67]. The database would include data on the time/place of entry, the length of stay authorised as well as biometric data of the persons registered. In case of "overstayers", the system would transmit automated alerts to the competent authorities. (b) The granting of a **Registered Traveller Status** to "low risk travellers" from third countries who after appropriate pre-screening could benefit from a simplified and automated border check. (c) An **Automated Border Control System** to manage entry/exit of both third country nationals (as far as they have the status of a registered traveller) and EU citizens.

The reception of these ideas has been mixed, critics notably pointing to certain discrepancies between the doubtful/alleged benefits of the monumental border control system proposed and the inconveniences in terms of fundamental privacy risks associated to such large-scale data collection (cf. Geyer 2008). Most of all, it appears doubtful whether the system really fulfils a facilitation need, given that neither EU citizens nor third country 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 your doorstep as possible. Sometimes these strategies involved just look-out posts or listening watches to capture the first signals of security threats approaching. When modern border management applies forward tactics, it will not be satisfied with a just passive monitoring of trends[69] but wants to do a pro-active job by possibly intercepting "undesirable elements" before they actually reach the own borderline. The relocation of controls may also be motivated by concepts of risk prevention, e.g. to prevent persons with a possible terrorist profile to board a plane.

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

The most common extra-territorial formality is the **visa application** which imperatively has to be complied with in the country of origin, residence or temporary stay of the applicant. The

---

[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 up to 3 months** (regardless whether they require a visa or not!), by far the largest group entering the EU. Exceptions would be granted to holders of local border permits, national long-stay visa or residence permits as well as all those exempted from stamping (e.g. 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.

requirements are insofar alike for visitors (subject to visa requirement) to Canada[70], EU[71] or the US[72]: 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.

Visa procedures take at the same time 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 other data will be run against watchlists (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 equally been inspired by the US example: so far, biometric data required for the **Visa Information System (VIS**), i.e. a digital photo and 10-digit-fingerprint[75] is to be collected, according to Article 48 VIS-Regulation, by the Member States consulates abroad[76] and subsequently to be entered by them in the VIS database. The information will thus be available in the system for identification purposes, once the visa holder will arrive at the external EU border (EU Commission 2008c). The situation would be different, however, under a possible future entry-exit system, for third country nationals not subject to a visa requirement: for them the necessary registration of biometric data will take place on the border at the occasion of their first entry into EU territory (EU Commission 2008b).

A clear signal in terms of keeping non-approved foreigners at distance is also found in the **electronic travel authorisation (ETA)** concept, practised for years already 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 "Electronic Travel Authorization program" in the US[78] and as „Electronic System of Travel Authorisation" (ESTA) 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.

---

[70] Visiting Canada: How to apply: http://www.cic.gc.ca/english/visit/apply-how.asp#step5

[71] Visas for entry into Germany: http://www.auswaertiges-amt.de/diplo/en/WillkommeninD/EinreiseUndAufenthalt/Visabestimmungen.html#t6

[72] Destination USA: Secure Borders. Open Doors. How to Get a Visa. http://www.unitedstatesvisas.gov/obtainingvisa/index.html

[73] Whereby a Schengen short stay visa granted to third country national allows him/her to travel in the entire Schengen area, and not just to the Member State which issued the visa. See EU/DE instructions on the Schengen area http://www.auswaertiges-amt.de/diplo/en/WillkommeninD/EinreiseUndAufenthalt/Schengen.html

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

[75] Art. 9(5) and 9(6) VIS-Regulation (EC) .../2008: currently available EP version (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 Article 48 of the Regulation

[77] It 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] cf. DHS (2006a)

[79] cf. EU Commission (2008b), p.9

> The United States in fact foresee the new mechanism just for those countries still enjoying visa-free travel under the VWP program (DHS 2006a) and the EU seems attracted by the same aspect (EU Commission 2008b). Labeled by 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" surfaces also 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 on 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, then Germany and Italy in 2004 brought up the concept of "off-shore solutions" in terms of so-called "**Offshore Humanitarian Processing Centres**" (Helmut 2005) which 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 centers are not new in global refugee policy; in the 1990s the United States was using its facility at Guantanamo base(!) in Cuba to process Haitians trying to make their way to the United States by boat. The Australians employed a similar idea in the wake of the Tampa crisis in 2001, creating processing centers for intercepted asylum seekers on the Pacific island nations of Nauru and Vanuatu (IRRI 2004).

Although first deportations from Italy had already started and the EU ministers of the 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 unique **Canadian approach**, which has been successfully adopted by others, to stop terrorists, criminals and other undesirables. In the recent years, Canadian officers abroad have stopped more than 33 000 people with false documents before they boarded planes for North America (FAITC 2003).

2.1.2 Further extraterritorial presence of control and law enforcement

Off-shore 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 if they can do the job on their own, relying on their expertise and skills.

---

[80] a service fee of 20 AUD (approx. 12.15 EUR) will be incurred for online lodgement (Australian Government 2008).

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

[82] Kroeger (2007)

The most prominent example is the post-9/11 **Container Security Initiative (CSI)** launched in early 2002 in 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, such as in the case of weapons of mass destruction (WMD), the CSI intends to anticipate the control of containers – which carry approx. 90% of international trade – outside the US territory (Koslowski 2006).

> The reasoning behind this strategy is that the detection of WMD after the 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 for the purchase and operation of refined technology are immense as well as the funds necessary for the running of the human interface, but they are "many times outweighed by the cost to the U.S. 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 (EU Council 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 will show that positions are not that far apart as one might believe from the EU-US clash on the air security MoU currently proposed by the US to the 27 Member States (Traynor 2008). In fact, the new Regulation on Civil Aviation Security (EU Parliament 2008) expressly allows Member States to authorize 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") which 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]; this practice widely outlawed was adopted by US intelligence services in the 1990s in order to "counter terrorist threats more efficiently". As opposed to "legal rendition" this refers to a form where 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 (cf. Geyer 2007). This practice as well as 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% containers was the normal share in major ports; afterwards this ratio has improved whereby no exact figures are given; however the ratio of presreening has raised to 100% and there are now refined methods of risk assessment, cf. McClure (2007)

[84] for further details on the proposal see ... below 2.3.1 New generation of commitments

[85] cf. Geyer (2007), p. 2

[86] „EU countries ignored CIA terror suspect flights, report says", The Guardian of 14 February 2007. http://www.guardian.co.uk/world/2007/feb/14/eu.usa

2.2 Legislative hot spots: some crucial aspects in designing PNR mechanisms

Clearly the drafting of legislation on PNR and its sensitive surroundings involves touching quite a number of hotspots, i.e. legal and ethical issues whose handling would require an in-depth exam[87]. In most cases this will occur within the regular discussion on legal and practical features of existing and planned instruments.

There are, however, two items with a more remote significance but still important for the actual shape which PNR legislation obtains 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) created or reaffirmed some of the well-known stereotypes of the 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[88].

This same scenario under the motto "Americans are from Mars and Europeans are from Venus"[89] is likely to arise anew with our current privacy subject: the "old Europe" with its strong sensitivity towards privacy intrusions by means of collecting, processing and transmitting passenger data[90], in 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"[91]. The formula is catchy but it is also one-sided - given that the situation is just the other way round in a related area.

It is the merit of Rey Koslowski of the University at Albany, well-reputed expert on "Border Control and Homeland Security in the Information Age" and a frequent witness in this matter at

---

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

[88] cf. 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."

[89] Motto taken from Robert Kagan's book „Of Paradise and Power: America and Europe in the New World Order" (2003)

[90] cf. 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 Hustinckx has warned the Google corporation to expand its 360°, full-colour "Street View"-map service to Europe, because this might lead to expensive lawsuits for privacy violation. EU Observer of 16 May 2008, http://euobserver.com/9/26154/?rk=1

[91] Cf. Paul Rosenzweig, Deputy Assistant Secretary at DHS, on the EU draft Framework Decision on data protection in police and criminal matters: *" 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 Statewatch http://www.statewatch.org/eu-dp.htm

US Congress hearings, to have pointed to a surprising link between the well-known toughness of US border policies and a less known inefficiency in establishing alternative control mechanisms inside 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"[92].

> 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, carry ID-cards that the police may ask to see any time. Also at the workplace there are checks, work permits are required and enforced, and employers will be tightly controlled.
>
> In the US in contrast, once that migrants have crossed the border they will rarely be stopped any more.

In the US – as well as in practically all other common law countries – it has, despite several attempts by the Bush administration, not been possible to launch a halfway promising campaign in favour of a national ID card. Despite 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 try.

> 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 kind of central authority, even their own government: for some, ID-cards represent an evil per se, "symbol of a 'papers-please' society reminiscent of Nazi Germany and Stalinist Russia"[93]. The suspicion turns even against a legislative bill to introduce national driver licenses because they might "result in a national ID card that compromises privacy"; 6 US states have already rejected the federal project, and it seems unlikely that it can be realised (Frank 2007).

Although emotions did not seem to heat up quite as much 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, provide proof on residence etc include a combination of official and private documents such as drivers licenses, birth certificates, electricity bills etc (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 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 ID-card mechanism is not everyone's preference and that there strong traditional objections to such approach in the anglo-saxon/common law world, international discussions should take into account that the difficulty in "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!

---

[92] Koslowski (2006), p. 92

[93] cf. Neal Kurk, Republican state representative from New Hampshire as cited by USA-Today in June 2007 (Frank 2007). Similar statements are available in great numbers from other parts/groupings in the US and Canada.

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

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

Although the PNR concept originally stems from the North American tool set, one might imagine that the EU after so many years of intense cooperation would have installed its own set-up to take advantage of a system which runs anyway and produces which could be retrieved with a simple snap of finger. However, the EU is not yet ready for it, although the US has promised reciprocity already in its undertakings under the 2004 agreement[94].

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

While – with the current trend towards tighter security approaches in Europe – it can be expected that the **EU PNR scheme** will be operational not too far from now, the 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 loosing access to American airports continued to accompany the transatlantic PNR negotiations ever since that moment. One cannot exclude that certain clauses accepted by the EU negotiators and later on bitterly criticized by privacy commissioners would not reconsidered/renegotiated if the EU had been somewhat more at ease in these circumstances.

The question many observers raised with astonishment was why the EU has shown and still shows such unease and haste about quickly coming to terms with the United States?[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 was feared, however, that retaliation measures of such fundamental dimension would not be understood by the European citizens who wanted – according to a somewhat doubtful assumption - above all to enjoy continued and unimpeded travel to the US.

The same psychological mechanism plays within the closely related area of the US Visa Waiver Program (VWP) and its conflict with basic features of the EU visa policy: again it is a somewhat half-hearted negotiation style which handicaps the successful implementation of a confirmed EU policy position.

---

[94] Para 45 of the Undertakings by CBP of 11 May 2004 (DHS-CBP 2004)

[95] This already for the first official statement in terms of the Commission Communication of December 2003 (cf. EU Commission 2003). However, as regards the biographic data under the API scheme, Directive 2004/82/EC already authorized Member States the request such data from airlines and run it against JHA databases such as SIS (cf. EU Council 2004)

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

[97] EU Parliament and Council (1995)

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

According to the solidarity provision of Article 1 (4) Regulation (EC) 539/2001)[99], Member States exposed to a visa requirement by a third country may invoke the solidarity of all 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 to make use of the solidarity clause[100]. It seems that also 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 for sure 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 for ever want to tolerate such deprived situation. The consequences have become 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 VWP. In defiance of the Commission call for Union discipline, the Czech Republic and others immediately declared their interest in such arrangements, last but not least 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 recognize that defending European convictions in 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? The answer is open/uncertain and definitely not worth to abandon a good negotiation argument for it.

2.3 PNR and resistance to excessive intrusion

While "resistance" makes allusion to times of foreign occupation and totalitarian regimes, the term has become more and more common in recent years to describe an attitude towards a growing tendency of "replacing the law in counter-terrorism practices across states" (Bigo 2006). Resistance in this sense takes place not in a clandestine fashion, but by individuals and organisations which in one way or the other take part in legislative decision-making, implement/apply existing legislation or in shaping public opinion.

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

2.3.1 Government institutions

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

---

[99] EU Council (2001)

[100] The same situation exists for Greece which the US authorities had always considered as too little reliable to join VWP, Siskin A. (2005), p. 19

[101] cf. Czech Interior Minister Ivan Langer who 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 an slave of the European Commission." EuroNews of 28 February 2008, http://www.euronews.net/index.php?page=europa&article=472497&lng=1

In both, the **US and Canada**, the post 9/11 counter-terrorism legislation (USA PATRIOT Act and Canadian Anti-Terrorism Act) as proposed by governments received almost unanimous support by the respective legislatures[102], despite serious objections for incompatibility with fundamental rights having been voiced by civil rights groups and other critics. In 2005/2006 when the respective acts had to be renewed, a considerable difference became visible between both 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 **European Union**, even governments – despite many avowals of solidarity – were initially hesitant to pick up the pace of change adopted by the US (cf. 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 (cf. Fraser 2007). With the 2005 Hague Programme, the Prüm Treaty of the same year and its inclusion into 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 are rapidly approaching the closer 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, by a highly critical resolution of July 2007[106], the new instrument with the US as "substantively flawed"[107] Also at the Member State level, parliaments remained critical and vigilant, above all the UK House of Lords with its extremely detailed PNR report in preparation of the 2007 EU-US agreement[108]. But also other parliaments left traces, that they closely look at such proposals and take the trouble to stand up against their governments when they see human rights violations[109].

---

[102] cf. Cf. "USA PATRIOT Act " Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/USA_PATRIOT_Act"Canadian Anti-Terrorism Act" Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Canadian_Anti-Terrorism_Act

[103] Such conclusion may be drawn from statements by national politicians who increasingly tend to „think the unthinkable" with regard to counterterrorism in terms of abandoning established democratic and legal principles such the distinction between internal and external security, presumption of innocence etc (Spiegel 2007 reporting on some „excursions on dangerous terrain" by German Interior Minister Schäuble).

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

[105] http://www.epractice.eu/document/873

[106] EU Parliament (2007)

[107] see EurActiv of 13 July 2007 http://www.euractiv.com/en/justice/parliament-slams-pnr-deal-substantively-flawed/article-165524

[108] House of Lords (2007)

[109] just to cite two examples from the German Bundestag and the Czech Republic, see http://dip.bundestag.de/btd/16/048/1604882.pdf and http://www.edri.org/edrigram/number5.15/czech-pnr-reservations

2.3.2 Jurisdiction

The **jurisdiction** 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 merits in the specific PNR field: the European Court of Justice profoundly disappointed the European Parliament as plaintiff in the Joint 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 breach of fundamental rights[111]. As a deplorable consequences of the decision, (1) PNR data when used for counter-terrorism purposes does not benefit anymore from privacy protection under Directive 95/46/EC any more but finds itself in a legal void due to the lack of a 3rd 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" (House of Lords 2007, p. 22).

2.3.3 Data protection authorities (DPAs)

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

In **Canada**, the federal 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 CCRA)[112]. A second victory for privacy interests is seen in the additional "commitments" made by the new Canadian Border Services Agency 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 were less successful, notably in the case of the Passenger Protect Program/"no-fly" list of 2007[115] when a joint resolution by all privacy commissioners was simply not taken account of. The current review of the Privacy Act of 1983 is seen as a test case to what extent 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 (Art 29 WP) which deal exclusively with airline passenger data[117]. This accounts for approx. 10% of the report volume produced by the working party and is on top of the interventions by the

---

[110] e.g. the acquittal of 9/11 suspect al-Motassadeq by the German high court BGH because for reasons of counter-terrorist strategy he was deprived of taking advantage of his full rights under the criminal procedure act; cf. Brimmer (2006); Der Spiegel of 2 March 2004, http://www.spiegel.de/panorama/0,1518,289065,00.html

[111] EJC Judgment of 30 May 2006, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79939469C19040317&doc=T&ouvert=T&seance=ARRET

[112] see OPC press release „Breakthrough for Privacy Rights"of 9 April 2003 http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp

[113] cf. Opinion 1/2005 (Art 29 WP 2005)

[114] Letter of 5 May 2008 from OPC (C. Baggaley) to the author

[115] see section ... above

[116] see Statement by Privacy Commissioner Stoddard of 29 April 2008, http://www.privcom.gc.ca/parl/2008/parl_080429_01_e.pdf

[117] for a complete list of opinions/reports of the Art 29 WP see http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

European Data Protection Supervisor Peter Hustinx. The opinions and their undeniable impact on policy-making will be covered in more detail within the legal analysis of the respective instruments.

2.3.4 NGOs and others

Besides "data protectors", it is mainly civil liberties NGO's[118] and monitoring services such as which contribute to raising public awareness of privacy intrusions. Both Statewatch, EPIC and Privacy International entertain specific observatories on airline data[119].

> Airline resistance is mainly inspired by the legitimate interests of trade to avoid 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 refer 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 throw a closer look on the individual instruments to see to what extent they conform to the legal frameworks created at the national and international level.

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 – as indicates its name and provenance – is not in 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 OECD, ranging from „collection limitation" to „accountability", seem to please every one, 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 to what extent the terminology diverges between the various national and regional implementations of the OECD Guidelines: confusion starts within the guidelines whose section headers („labels") are not always representative for what the section contains.

> E.g. Section 7 labelled „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 know about it. Others wishing to adapt the OECD rules to academic or practical purposes left the principles unchanged but attach entirely different labels to them (Shimanek 2001)[121]. The most common "implementation mode", however, is to (1) redraft

---

[118] for a comprehensive listing of privacy organisations and other resources see EPIC's „Online Guide to Privacy Resources" http://epic.org/privacy/privacy_resources_faq.html#Privacy_Organizations

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

[120] see OECD (1980)

[121] e.g. „Notice", "Purpose", "Consent" , "Security", "Disclosure", "Access", and "Accountability"

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

Implementation instruments again found different structures and organization principles to reproduce 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 correspondance linking the various terminologies.

The present paper will therefore try to find a pragmatic way to appropriately weight 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 recognized privacy rules

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

Given the prominent role of Article 29 Working Party[123] in accompanying all PNR instruments so far discussed or adopted, notably by providing detailed opinions at the various stages of 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 utilization 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 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 list is available in PIPEDA of 2000, whereby the latter act formally applies to private-sector data issues only. In practise, Canadian privacy commissioners loosely refer to "fair information principles and practises" (FIP's) and Global Privacy Standards[125] as accepted at the international level[126]. Furthermore, Canadian privacy experts have become widely familiar with the EU nomenclature – especially since the Art 29 Working Group, with its opinions, exercised a decisive influence on the final outcome of the EU-Canada PNR negotiations[127].

---

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

[123] 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 (EU Parliament and Council 1995)

[124] cf. ECJ (2006)

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

[126] 28th International Conference of Data Protection and Privacy Commissioners (2006)

[127] Letter of 5 May 2008 from the Canadian OPC (C. Baggaley), underlining the importance of Art 29 WP's opinion 1/2005, all the more as the OPC was not invited to participate in the negotiations.

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

a. Recognition of data protection 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 (Art 29 WP 2004),

b. Transitional character of adequacy findings: in view of rapidly changing threat scenarios in the case of terrorism and trans-national crime, data flows should not be authorized for an undetermined period but made subject to a "sunset" limitation.

c. Basic data protection principles ("content principles")[129]

    1. 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.

    2. 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.

    3. 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.

    4. 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.

    5. 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 he/she should also be able to object to the processing of the data relating to him/her.

    6. 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[130]

    1. good level of compliance with the rules

    2. support and help provided to individual data subjects

    3. appropriate redress provided to the injured party

---

[128] Art 29 WP (2004), section 2

[129] cf. Art 29 WP (1998), p.6

[130] ibid p.7

3.2 Evaluation of the EU -Canada agreement of 22 March 2006

The "model boy" 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.

> The Art 29 Working Party has delivered two detailed opinions on the level of protection granted to PNR data in Canada (3/2004[132] and 1/2005) in addition to an opinion by the European Data Protection Supervisor on the proposed agreement as such[133] – whereas other bodies 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[134]. However the MEPs conceded that content-wise the agreement represented an "*acceptable balance*".

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 "light weight" position within the EU legal order but on the contrary an important pillar of the legal order which may be subject to restriction only if a similarly important interest is at stake (Art 29 WP 1998).

In the case of PNR, the value at stake is the "fight against terrorism" which routinely is accepted as a sufficiently developed counterweight, since it represents "both a necessary and valuable element of democratic societies" (Art 29 WP 2004). However, in this context terrorism does not stand on its own, it is combined – just as in the case of the 2004 EU-US agreement - with the much wider field of "terrorism-related and other serious crimes, including organized crime, that are transnational in nature"[135].

This is in sharp contrast with the Commission adequacy decision which solely refers to the Community's "commitment to supporting Canada in the fight against terrorism"[136]. Surprisingly not even the normal "watchdogs", the Art 29 Working Party as well as the European Data Protection Supervisor (EDPS), take any offence at this, neither at the divergence between adequacy finding and the actual agreement text, nor at the diffuse concept of "terrorism-related and other serious crime" which leave room to a wide spectrum of interpretation.[137]

> In its first opinion, the Art 29 WP still had expressed serious doubts as to these "too widely defined purposes" (Art 29 WP 2004, s.6), but dropped this charge in early 2005, without any significant amendments having been made to the text[138]. Only the UK House of Lords

---

[131] ePractice.eu (2005)

[132] Art 29 WP (2004)

[133] EDPS (2005a)

[134] EU Parliament (2005)

[135] cf. EU-Canada PNR Agreement (2005), 1st recital

[136] EU Commission (2005b), 8th recital

[137] cf. Art 29 WP (2004), Art 29 WP (2005) as well as EDPS (2005a)

[138] Art 29 WP (2005), s.3

> remained sceptical of the delicate aspects of this formula[139] 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 the proposal for an EU PNR system of 2007[140] - leading to the simple question, "how serious must a crime be to fall within this description and so be covered by the PNR Agreement?" (House of Lords ibid.).

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 that of purpose limitation and onward transfer: crimes other than terrorism are likely to bring in entirely different sets of authorities concerned which in turn widens the scope of those getting in touch with the data in question (see section 3.2.3.6 below). At this stage, the question should be kept in mind whether a positive list of "serious crime" categories (loosely inspired by the model of the European Arrest Warrant[141]) should be agreed - best at a multilateral level – to avoid serious inconsistencies in international privacy protection.

3.2.2 Transitional character of the adequacy finding

DP 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 case of major change, any such arrangements should therefore be time-limited (Art 29 WP 2005, s. 3), best 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 (Art 29 WP 2004, s. 3).

The agreement fully complies with this requirement by foreseeing (1) in its Article 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 Article 7 of the Adequacy Decision that the decision expires after 3.5 years if not extended before.

A continuous monitoring of the agreement and its operation is ensured by the Joint Committee under Article 6 of the agreement, which is in charge of settling possible disputes (Article 7) and organise the Joint Reviews (Article 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 follows:

3.2.3.1 Purpose limitation

Both Commission and EU data protection authorities have positively expressed their satisfaction that PNR data transferred from EU air carriers to Canadian 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; other serious crimes, including organized crime, that are transnational in nature."[142]

---

[139] House of Lords (2007), paras 104 ff

[140] EU Commission (2007a)

[141] cf. Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA)

[142] EU Commission (2007a), 15th recital; Art 29 WP (2005), s.3; EDPS (2005a), s.4.3

However, doubts remain to what extent such wide formula may be considered an effective "purpose limitation": one might just refer to the initial comments by the Art 29 WP which criticized 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."*[143]

Between the first and the second intervention by Art 29 WP, 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 Art 29 WP 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 had a "clear relationship with terrorism".[144]

3.2.3.2 Data quality and proportionality

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

- **Limited list of categories**[145]

The particularly lengthy list of 38 data categories[146] initially required by CBSA was reduced to 25, in particular by eliminating so-called "open categories" which could reveal sensitive information on the passengers. Remaining doubts by 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 via push-system only**

A major achievement was the exclusive adoption of the "push-method" which allows airlines to keep control over the data transfer (cf CBSA 2005a, s.7)

- **Enhanced data quality**

Last but least due to own painful experience (cf Maher-case[147]) Canadian authorities subscribed to two important commitments, ie (1) to apply no change to PNR data obtained, and (2) collect additional data to supplement PNR data only through lawful channels (EU 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 poor data quality of enforcement databases and watchlists.

---

[143] Art 29 WP (2004), s.6

[144] EU Commission (2005b), Annex 'Commitments by the CBSA', s. 2

[145] cf. Annex II of the agreement (EU – Canada 2005)

[146] a list „well beyond what could be considered adequate, relevant and not excessive", Art 29 WP (2004), s.6.3

[147] for details on the Maher case see p. 8 above

- **Reduced retention periods**

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

Following considerable concessions made by CBSA, the maximum retention period was reduced from 6 to 3.5 years, with name data being accessible after the initial 72 hours period only in very exceptional circumstances (CBSA 2005a, s.8).

3.2.3.3 Transparency

As a primary element of transparency, the Art 29 WP requested the Commission to include a "full picture of the relevant Canadian regulatory framework, … as an annex to the Commission Decision" (Art 29 WP 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.

> In basic terms, the API/PNR programme was set up in 2001 by the predecessors of 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 Sections 148(1)(d) of IRPA allowed the government, by means of the Passenger Information (Customs) Regulations, to require the provision of API/PNR data prior to the arrival in Canada. IRPA as amended by Bill C-17 allows for information sharing arrangements with other Canadian agencies[148].

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 (CBSA 2005a, s.21). Furthermore the Commission adequacy decision provides clear instructions as to the circumstances under which the data flow to Canada is to be suspended by Member States (EU Commission 2005b, Articles 3, 4).

3.2.3.4 Security

EU data protection authorities excel in praising the technical and organizational security measures taken by Canadian authorities (CBSA 2005a, s.33 ff) 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 in 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). CBSA has therefore agreed, in section 31 of the commitments, to allow EU residents to initiate a complaint via their national data protection authorities which was considered a satisfactory solution (Art 29 WP 2005, s.3.6.1).

It is underlined by the EU DPA's that the agreed redress procedures – just as all the other commitments made by the Canadian authorities – are based on legally binding engagements

[148] cf. Art 29 WP 2004, s.5; for the Canadian legislation cited, see Bibliography – List of legislation, p. 66.

which distinguishes them positively from similar arrangements taken with the United States (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. Also the Privacy Commissioner is empowered under the Privacy Act to commence an investigation in respect of the disclosure of personal information (CBSA 2005a, s.35).

3.2.3.6 Restrictions on onward transfers

The issue of onward transfers as regulated by CBSA again meets with full approval by the EU DPA's[149], since according to the commitments (1) transfers/disclosures will never be made in bulk but decided on a case-by-case basis. (2) There will be no online access granted to other authorities. (3) Disclosures will depend on the condition that (a) they are relevant to the other agency, (b) respect the purpose limitation referred to under 3.2.3.6. above, and (c) the recipients undertake to afford it the same protection (CBSA 2005a, s.12 ff). Similar safeguards apply to the disclosure to other countries (ibid s. 16 ff).

The only doubt that remains over this perfect construction concerns the imprecise purpose limitation which we have already denounced under section 3.2.3.1 above. Vague terms such as "serious crimes", with their strong risk of diverging interpretation, 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 have been extensively appreciated by the EU DPA's: this is due to (1) the advanced technical and organizational security measures discussed under 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 the compliance with the law (cf. section 3.2.3.5 above).

3.2.4.2 Support and help provided to individual data subjects

Citizens take first of all advantage of the general transparency principle, requiring 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 (cf. 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 as fully appropriate – are described in more detail in section 3.2.3.5. above.

---

[149] Art 29 WP (2004), s.6.5; (2005), s.3.5; EDPS (2005a), s

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 to agreements signed on the same subject with the United States. Besides 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 which takes up its responsibility to protect citizens to an utmost degree from undue privacy intrusions which may occur during the operation of PNR mechanisms.

3.3 Comparative overview of other major PNR instruments[150]

The comparison between the EU-Canada agreement and other recent instruments will help to establish additional clarity as to quality of this "flagship" instrument; it will also contribute to identifying current tendencies in revised PNR concepts – possibly a signpost as to where the forthcoming EU - Canada negotiations will lead.

3.3.1 EU-US agreement of 2004

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

The EU-US instruments stand out already by the sheer number of critical comments they have attracted. This may have to do with the close scrutiny US action at the international level is traditionally exposed to. However, such scolding does not exclusively come from those who frequently pinpoint US human rights violations in the context of Iraq, FBI/CIA intrigues, Guantanamo/El Ghraib prisons. There also are highly reputed bodies such as the House of Lords EU Committee which strongly warn against undesirable trends developing in PNR negotiations with the United States[151]. 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 was true that in the case of Canada that 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 lavished the negotiation parties with good advice and admonition - and were regularly disillusioned to see that their detailed opinions had all had been in vain. The European Parliament, after its objections against the Commission 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, EPIC and Privacy International which remain practically silent on the Canada agreement dedicate entire "observatories" on EU-US airline passenger data disclosure.

---

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

[151] cf 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 (cf. Article „Lords EU Committee Raise Concerns Over Passenger Name Record Agreement With US", http://www.libertysecurity.org/article1489.html)

This peculiar situation is maybe 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 into the details of airline passenger control. The "war" (as opposed to "fight") against terror, as seen by the US side, justified the use of uncommon means: at the latest by July 2003, the US ended the separation ("wall") between information obtained by the law enforcement and intelligence communities (Rees 2006, p. 82). This also allowed for a wider choice of options when looking at details of airline security risks. Europeans felt irritated not 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 sensitive area.

> European suspicion was particularly nourished by subsequent discoveries that – while official negotiations were in progress – US authorities had already been working on system changes incompatible with the results so far obtained (eg exploitation of PNR data by targeting devices such as CAPPS II, ATS, Secure Flight[152]). Negotiators were puzzled that the US delegation repeatedly came back with imprecise treaty language, blanket clauses etc inadmissible in terms of data protection (purpose limitation principle), and even the official EU Commission report on the joint review on the 2004 agreement complained that access to certain control records had been restricted by DHS due to reasons of secrecy[153].

In view of the volume of controversial items, the following review will confine itself to those aspects essential for allowing 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 be illustrated also in a quantitative manner: with regard to the 21 criteria applied by Art 29 WP to check privacy compliance, commitments by the US side[154] failed to comply with the rules in roughly two thirds of the items (14.5 = 66%)[155]. 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.[156]

Major items of concern were the following (in 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 balance of values may be assumed for counter-terrorism but not for the second purpose cited, ie "preventing and combating of … other serious crimes, …" which is considered "too vague" to be acceptable as a description of purposes (Art 29 WP 2004a, s.5B).

Item 2:Transitional character of adequacy finding

This item is formally complied with: there is a (1) "sunset clause" to terminate the adequacy decision/agreement if 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 Agreement (EU-US 2004), and (3) in the case of malfunctions, Member States may suspend the data flow according to Article 3 Adequacy Decision (EU 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 due to (1) certain records

[152] see section 1.2.3.1 above, p. 14

[153] EU Commission (2005), p. 6

[154] see CBP (2004)

[155] This refers to the final comments by Art 29 WP as laid down in Opinion 1/2004 (Art 29 WP 2004a)

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

> being denied to the review team for reasons of secrecy and (2) the technical impossibility for CBP to identify complaints/requests relating to EU PNR data (EU Commission 2005; Guild 2006).

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" (Art 29 WP 2004a, s.5E).

Furthermore the Working Party points to the following "blanket clause"-type of insufficiencies in the description of purposes:

- still no list available of the agencies authorized to receive data by means of onward transfer
- blanket clause allowing CBP, in its discretion, to forward data to any authorities, including foreign ones, with "law enforcement functions" (CBP 2004, s.29)
- blanket clause to allow data transfer "as otherwise required by the law" (ibid, s.35)

Specifically harsh criticism was passed 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 (Art 29 WP 2004a, s.3).

> The EU authorities became again concerned with the delicate aspects of such mass data processing , when they were confronted with 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[157]. For further details see section 3.3.1 below.

Item 3.2: Data quality and proportionality

- **List of data categories**

The final list of 34 data categories found no approval by Art 29 WP: it was considered excessive since (1) so far only 4 acceptable categories had been eliminated from the original proposal, while (2) sensitive items such as OSI/SSR containing information on special needs/preferences of passengers remained on the list (Art 29 WP 2004a, s.5C).

- **Transmission via push-system**

The outdated pull system allowing CBP to access airline computers and "pull out" the data needed remained in place wherever airlines were not ready yet 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 CBP would avoid pulling/using sensitive data as well as delete such data where accidentally pulled (Art 29 WP 2004a, s.5D; CBP 2004, s.9).

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

- **Data quality**

[157] ACLU (2007)

Deficiencies regarding data quality were seen in the fact that (1) the access to sensitive data was insufficiently blocked (eg pull system) and (2) that the "use of trigger words" to eliminate such data represented an inept solution (Art 29 WP 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.5 L).

- **Retention periods**

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

> The WP – at this stage – was not even aware of the effect, in terms of retention periods, of the processing of PNR data by the Automatic Targeting System (ATS): in this case retention was prolonged to 40 years!

Item 3.3: Transparency

The WP considered the CBP plans of informing the travelling public, via 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.5 J.1).

> The further issue of a complete description of relevant US legislation to be displayed in the Annex in the agreement/adequacy decision was not raised here (different from the discussion of the Canada agreement).

Item 3.4: Security

No specific remarks were made under this header: however, the multiple interlinking of PNR processing with other procedures (profiling, targeting etc) suggests that there may be "weak links" and loopholes putting at risk the security of the entire system.

From the organizational point of view, the fact that CBP officers were without guidance as to the notion "serious crimes that are transnational in nature" (EU 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 was authorized in exceptional cases only (ibid).

Item 3.5: Rights of access, rectification and opposition

Contrary 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 (FOIA) which may be opposed to the data subject when seeking 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 latter (CBP 2004, s.38).

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 CBP (ibid s.39) will work in practice (Art 29 WP 2004a, s.5 J.3)

Redress procedures as proposed by CBP were welcomed by the WP which at the time expressed doubts whether the "in-house" procedure involving the DHS Chief Privacy Officer as last instance, even regarding complaints against his own office, really represented an appropriate solution (ibid J.4).

Item 3.6: Restrictions on onward transfers

According to the WP, serious shortcomings in the area of onward transfers concerned mainly the (1) absence of a list of public bodies entitled to receive the data, and (2) the before-mentioned **blanket clauses in sections 29, 34 and 35 of the CBP** undertakings which leave a large amount of discretion in overriding the principles governing privacy protection in general and the present agreement in particular.

> According to this CBP may, in its discretion, forward PNR data to government authorities (including foreign ones) "with **counter-terrorism or law enforcement functions**" (s. 29); 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).

It is certainly no surprise that the Art 29 WP, 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" (Art 29 WP 2004a, Conclusion).

3.3.2 The interim agreement of 2006

After annulment of the 2004 agreement by ECJ decision of 30 May 2006, the parties had to act rapidly in order to establish a new instrument compliant with views of the Court.[158]

> Although the challenge from the EP was based on the claim that the Commission adequacy decision and the Council decision authorising the signature of the agreement were ultra vires, ie in breach of fundamental principles of Directive 95/46, 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: data processing operations for purposes of public security and in the context of criminal law were excluded from the scope of a 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 but find themselves somewhere in a legal "no man's land". In the absence of the third pillar data protection instrument still not accomplished the only protection may be deducted from the human rights norm of Article 8 ECHR (Guild 2006).

The first phase between termination of the 2004 agreement (taking effect on 30 September 2006) and entry into force of the 2007 agreement (end of July 2007) was governed by an **Interim instrument signed on 16 October 2006** (EU – US 2006). While the EU, in the interest of continued transatlantic air traffic, 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 Washington during the last couple of years" and that there were **new conditions added by DHS** as transmitted by letter from DHS Assistant Secretary Stewart Baker of October 2006[159].

This concerned notably the following elements:

- The Undertakings from the 2004 agreement were not valid any more in their original form but had to be read "as interpreted in the light of subsequent events" (HoL 2007, s.60).

---

[158] for details on this phase, see House of Lords (2007), p. 21ff

[159] the text of the Baker letter is reproduced as Appendix 7 of the House of Lords report on the EU-US Agreement (House of Lords 2007)

- 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 had now to be routinely shared with ISE agencies.
- Extension of PNR elements for transmission under field 11 (frequent flyer information) to cover all frequent flyer elements such as phone numbers, e-mail addresses etc as they "may provide crucial links to terrorism";
- Extension of access to PNR data "in the context of infectious disease and other risks to passengers", on the basis of Undertaking 34, whose extensive interpretation appeared justified in October 2006 due to the current risk of avian flu.
- Cancellation of the 3.5 years retention period: according to DHS, with the premature termination of the agreement also 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"* (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 allowing the party giving it to amend it 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 for the time to come, not only for the duration of the interim agreement but also the time after. If the 2004 agreement appeared backward oriented in comparison to 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 will have to have to examine to what extent this assumption applies to the 2007 instrument.

3.3.3 The 2007 Agreement

As a first impression it emerges that the **2007 EU – US Agreement** has been "stripped" of the procedural safeguards in terms of adequacy decisions, legislative role of the EP and the formal opinions by Art 29 WP and EDPS which faithfully accompanied the adoption of former PNR instruments. It is certainly worthwhile to retrace the "genesis" of the 2007 agreement (cf. Guild 2007) - last but not least to understand why the "successful" court action is rightfully referred to as a "Pyrrhic victory" (PI 2006), not only for the EP but the interests of privacy protection on the whole[160].

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 emphasizing 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 (cf. Undertaking 48 under the 2004 Agreement).

The next "surprise" arrived in terms of a letter from DHS to the Portuguese Presidency (DHS letter 2007) intended "to explain how …DHS handles" PNR matters in general and wishes to handle them with regard to the EU in future (cf. Guild 2007). It was made very clear that DHS

[160] cf Guild (2006) concerning the disappointing role of the ECJ in the context of PNR

did not wish to enter into discussions on these practices, but that the EU was just expected to take note of them *("We 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 three-fold components (agreement, DHS letter providing assurances about PNR privacy protection as practiced by DHS and the EU reply confirming that the level of protection was deemed adequate) is marked by two major tendencies, ie (1) the trend to unilateral influence to be exercised on the arrangements by the US side and (2) a considerable weakening of data protection safeguards (Art 29 WP 2007, p.2).

> In view of the focus of this paper being on EU – Canada relations, the evaluation of the instrument will be concise and confine itself mainly to highlighting the features which 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 which in the past had 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"[161]. From now on, the reviews will not take place annually but "periodically" and with the participation of only those officials/services who/which appear "mutually acceptable" (DHS letter 2007, article X), thus excluding inter alia DPA expertise and oversight as one of the "main pillars of effective protection"[162].

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 WP, the clause might be read in the sense that the future EU PNR system should not provide for level of protection higher than that of the 2007 agreement which would be conceived as a "very worrying development" (cf. Art 29 WP 2007, s.12).

In terms of individual privacy elements, the discussion follows the structure and terminology developed under section 3.2 above.

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 (DHS letter 2007, s.I.).

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

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

---

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

[162] Art 29 WP (2007), s.10; EU Parliament (2007), s.9

And after all it seems not even clear whether the DHS assurances will be published in the US Federal Register, condition for their becoming legally binding according to US law (Art 29 WP 2007, s.2).

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

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 WP, the clause might be read in the sense that the future EU PNR system should not provide for level of protection higher than that of the 2007 agreement which would be conceived as a "very worrying development" (cf. Art 29 WP 2007, s.12).

Item 3.2: Data quality and proportionality

- **List of data categories**

Appearances may be deceiving: when EU Commission and 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): since practically[163] all elements from 2004 had been retained, partially by regrouping them with others[164], and even a few elements were added, the list had even **increased from 34 to at least 37 elements** covered (Art 29 WP, s.5)

- **Push system**

Although the introduction of the push-system had been obligatory already under the 2004 agreement, DHS continued to employ the **pull-system** with direct access to airline computers at least in a number of cases. The 2007 DHS assurances mentioned 1 January 2008 as ultimate date for completing the move, but doubts remained whether this was a realistic assumption. Stumble stones could be that 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" (DHS letter 2007, s.VIII). Furthermore, as 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-system (Art 29 2007, s.5,7).

- **Retention period**

The DHS assurances also introduced new retention periods increasing the period from 3.5 to 7 years whereby another period of 8 years was added during which the data was "dormant" (DHS letter 2007, s.VII). DPAs complain about this "highly worrying" result of **18 years retention,** not compatible with recognized privacy standards (Art 29 WP, s.9).

Item 3.5: Rights of access, rectification and opposition

The rights of data subjects remain vague, last but least due to the uncertainty about the legal character of the "assurances" whether they confer formal rights or not (EU Parliament 2007,

[163] the only element deleted was „go show information"

[164] e.g. the former items „12 Travel agency" and „13 Travel agent" became item „10 Travel agency/ travel agent"

s.6). As a positive step, DHS extended administrative Privacy Act protection to non-US citizens/residents (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) means that a considerable number of additional agencies may have a "legitimate" interest to access PNR data, and (2) the abolition of the "case-by-case" requirement for such transfers. This might mean that PNR data might 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: already by letter of 30 July 2007, 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 DHS, the Council readily confirmed that the "EU shares your understanding regarding the **confidentiality of the negotiation process**" (Statewatch 2007b).

And on 15 August 2007, DHS announced a first **change to US privacy provisions** having an important impact on the protection granted to airline passengers. 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 and the 2007 Agreement together with the surrounding negotiations definitely confirms the impression that at the latest with the annulment of old 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 rule of law were given up, without even seriously trying to oppose the often one-sided US requests. And the hope is deceptive that the US needs/desires will be satisfied once for all – as the continuation under the following section will show.

3.3.4 A new generation of PNR commitments: bilateral arrangements between US and certain Member States

Starting from early 2008, additional US security needs were invoked on yet another front, ie 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 which were not covered by the EU-US agreement, the Member States were offered prospects of becoming part of the Visa Waiver Program (VWP). This involved the fulfilment of multiple conditions in terms of cooperation with the US such as allowing armed sky marshals on board of US-bound flights, provision of PNR data beyond the 2007 requirements, eg regarding passengers not landing in but overflying 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. However, all warnings by the Commission that Member States should avoid weakening the EU bargaining

position were in vain: the Czech Republic acting as a forerunner ("Trojan horse"[165]) signed the proposed Memorandum of Understanding[166] on 26 February while others followed in the weeks after (Estonia, Latvia, Lithuania, Hungary, Malta, Slovakia)[167].

> The solo advance by the 2004 newcomers although widely seen a nonsolidary act 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[168], the EU institutions did not act energetically enough to defend the interests of the new members. "There was no help, no solidarity from Brussels"[169]; 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 off 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 United States, 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" (Traynor 2008).

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 Electronic Travel Authorisation (ETA) question (Goldirova 2008).

Despite this temporary relief, perspectives remain modest and one might again think of a "Pyrrhic victory" for all 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 DHS whether they fulfil the expectations in "carrying out the security commitments" in question. Even if once designated as a VWP country, the Member State in question would have to undergo periodic examination at least on a biannual basis in order to retain the status (section A.2. of the MoU of 26 February 2008). In addition, what these countries might gain by fulfilling the conditions, will not be visa-free travel "old style" any more, but be subject to the ETA requirement which many consider just "a visa in disguise" (Goldirova 2008).

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 which are far from being resolved.

In view of the meagre results recently obtained and the visibly decreasing efficiency in achieving acknowledged privacy standards, in transatlantic one should dare to ask the basic question of what needs to be done in order to get back on track. Without entering into the details, it is primarily one point which seems to have unbalanced the negotiation concept.

---

[165] Pospísil (2008)

[166] for the complete text see Czech Republic – US (2008), http://www.vlada.cz/scripts/detail.php?id=31921

[167] Goldirova (2008a)

[168] cf. Regulation (EC) No 851/2005

[169] Traynor (2008)

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 – differently from the negotiations with Canada – did not manage to substantially influence the text finally agreed, this 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 leads to the further question of why EU delegations constantly convey the opposite attitude, that Europe **could not live without** such agreement – no matter how unfavourable the conditions are under which it is concluded. This unbalanced scenario occurs not only in PNR negotiations but equally 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 agreement. Or in Visa Waiver/ETA discussions one might consider to retaliate by equally introducing a visa requirement for US citizens. Is it too daring an assumption to suppose that Americans would suffer as much from such situation as Europeans?

In the end one could expect that US delegations 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 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"* The criticism is in first place addressed to the draft Framework Decision on data protection in police and criminal matter, since it *„seeks to apply the same tired, failed standards of adequacy that it has applied in its commercial laws."*[170]

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. All by itself, PNR processing is "worth nothing", not even capable of achieving the most modest operational success; still governments are ready to pay a high price in terms of delicate intrusions in 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 to what extent 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: besides making associations between known and unknown people, the main purpose of PNR is to contribute to a more precise risk profiling and targeting of suspects[171]; according to the profiles established border services can allocate their resources to specific hot spots on the border line. Furthermore the processing of PNR data is conceived to ensure seamless entry/exit controls via an improved coverage of all travel cross-border movements.

---

[170] statement in November 2007, cf Statewatch news http://www.statewatch.org/news/

[171] EDPS (2008)

4.1 PNR and border-related securitization: the direct impact

Evidence on direct hits achieved by PNR processing is extremely meagre. It is understandable that governments when asked to provide evidence on the value of PNR collection are getting into difficulties. This has first of all to do with the ancillary character of this type 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 the following statements (HoL 2007, s.19-21:

> - 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 EU Commission (DG Justice, Liberty, Security) mentioned several cases regarding terrorism/serious crime reported to him by the American partners, though sometimes only in outline, which proved the benefits of 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 which resulted from data collected by PNR; while giving examples of how the analysis of PNR data had prevented dangerous individuals from entering the United States. However, only one of the eight cases cited concerned terrorism prevention.

Whilst 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."* (ibid s. 22)

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 went wrong: besides the widely known example of Senator Kennedy stopped several times at US airports because of a mismatch with an entry on a no-fly list[172], this concerned the tragic example of Maher Arar, a Canadian citizen of Syrian origin who spent almost a year in a Syrian prison cell due to false conclusions drawn from correct PNR data by US and Canadian enforcement authorities[173].

Such regrettable errors in terms of „false positves" may arise from bad quality of the original PNR record (eg misspelled names), but more frequently from careless management of watch lists or no-fly lists against which PNR data are matched[174]. The same applies to situations in which too many authorities are involved in use/processing of the data or where system changes occur rather frequently.

---

[172] cf „Sen. Kennedy Flagged by No-Fly List", Washington Post of 20 August 2004, retrieved from http://www.washingtonpost.com/ac2/wp-dyn/A17073-2004Aug19?

[173] For a detailed description of the case, see Part 1.1.2.1 above

[174] cf. „Terrorism Watch List Is Faulted For Errors", Washington Post of 7 September 2007. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601386.html; see also Art 29 WP (2004a), p. 13

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 rapid sequence of newly tested screening or targeting devices, a growing number of watchlists as well as the strongly increasing 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 overstayers. In the following, the concept of complete control has not just survived the 9/11 events, it has gained additional momentum by the new counter-terrorist purposes under which the knowledge of "who's in and who's out" obtained 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 which will allow to trace movements and facilitate the pinpointing of suspects for easier apprehension.

However, this vision seems to suffer from a series of technical/organisational difficulties which 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 overly ambitious project.

Not much has changed since the conclusion drawn by the 9/11 Commission that "more than a half million persons enter the United States illegally across the many thousand miles of land border every year"[175]. Attempts to secure the Mexican border by means of fences, including "virtual" ones based on watchtowers, electronic detection devices and cameras, did not attain the results expected[176]. Also the lakes and rivers between Canada and US offer ideal opportunities for illicit crossings, especially if one mixes on a sunny day with Michigan's thousands of recreational boaters on Detroit River (Koslowski 2005, p. 23).

But loopholes are not only found on the **"green" and "blue" stretches of the border** line, also heavily guarded and equipped **ports-of-entry** prove vulnerable for various reasons (Koslowski 2005, p. 28, 39ff).:

(1) The immense **volume of approx. 330 million visa and US-VISIT-exempt travellers per year** (US and Canadian citizens, 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/exits per day** (San Ysidro/California-Mexico as well as Ambassador Bridge/Michigan-Canada) impeding 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 to biometrics to ensure identity verification of every passenger. There are

[175] as cited by the House of Lords (2007), s.106

[176] cf. „$20M 'fence' scrapped for not catching enough illegals" CNN International of 23 April 2008. Retrieved from http://www.printthis.clickability.com/pt/cpt?action=cpt&title

easy ways to "fool" RFID border systems[177] as well as digital fingerprint devices (eg via "fake fingers"[178]).

The overall construction of such an integrated entry-exit system is extremely complex, involving beyond advanced technology also important physical border infrastructure investments. Experts emphasize that the decision for a 100% completion of the system is last but not least a budgetary one. Are the President and Congress willing to expend sufficient financial and political capital to overcome these barriers? (Koslowski 2005, p. 63).

These lessons should be kept in mind wherever else, Canada as well as the EU, the introduction of such integrated border systems is being considered. Whereby such advice applies to the overall system as well as individual components, such 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, PNR is not more than a little though precious pearl among many on that long chain of elements called public security - even when looking at it only under the narrow angle 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, it requires the permanent exchange/matching with other sources to produce significant results - which represents at the same time its strength and its vulnerability.

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

The PNR story has thereby not been an isolated event but perfectly fits into overall securitization strategies *(*extraterritorial controls, biometric features, comprehensive system of entry-exit controls etc) which, besides tightening border security right at home, set up an advanced border line 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, the historic perspective reveals the extraterritorial - 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 inside the territory. Continental European 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 parliamentary and judiciary level but most of all DPAs which do not all agree with the overall approach taken in PNR matters.

---

[177] Under the NEXUS and SENTRI programmes, the enrollee receives a radio frequency (RF)-enabled proximity card. The RF-enabled chip on this card is read at the port-of-entry and 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)

[178] ibid p. 42

When testing the EU - Canada agreement and its **legal compliance** ("Acceptability") with accepted international standards of privacy protection such as the OECD guidelines and Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) it emerged that this instrument justly deserved its reputation as an "island of peace within troubled waters": besides a few partial objections, the overall system was extremely balanced and granted citizens appropriate protection and means of redress in case of intrusion.

Such judgment was all the more remarkable as it contrasted strongly with corresponding agreements concluded with the United States. While the Canada instrument showed an extremely low divergence rate from international standards (1.5 out 21), the 2004 US agreement failed to meet these benchmarks in more than two thirds of categories including vital issues such as purpose limitation, transparency, proportionality, retention period and appropriate citizens' right for access, rectification and redress. Instead of improving this score even degraded for the following agreements of 2006 and 2007, mainly due 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 EU-CAN 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 remain gaping wide open, especially to those who tend to disguise their movements, there seems not much sense in investing too much neither money nor policy-wise.

It is well to remember these considerations: due to the sunset clauses, typical for good privacy-related legislation, EU - CAN is soon due for a complete overhaul. In view of pro-security/contra-privacy tendencies currently visible even in Canada (e.g. no-fly provisions under Passenger Protect Program) and the EU (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 EU - Canada, instead of being a model for PNR legislation to come was sacrificed to short-sighted enforcement considerations.

Policy recommendations

Based on the results established in this article, the following policy recommendations are put forward:

- The exploitation of PNR data for counter-terrorism purposes represents a highly sensitive matter which 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/sacrificed for reasons of mere administrative/enforcement convenience. Any restriction must be carefully weighed in accordance the international data protection standards.
- As PNR data unfolds its potential for operational success as well as momentous errors only in the framework of mass data processing and 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/further extension of the PNR system should be preceded by a thorough analysis of the benefits the measures are allegedly expected to produce. The argument of an "increase of border security in general" should thereby 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/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 regarding the adequacy of protection.
- The EU – Canada 2006 agreement representing an instrument beyond (almost) all criticism, forthcoming review talks should definitely see to extend the validity of its existing provisions rather than aligning them to the doubtful standards of other recent instruments.

References

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

ACLU (2007), EU-US PNR Agreement in light of "Automated Targeting System", letter to European Parliament of 9 January 2007. Retrieved from http://www.privacyinternational.org/issues/policylaundering/ats/cavada.pdf

ADL (2004), *Canada and terrorism*. Retrieved from http://www.adl.org/Terror/tu/tu_0401_canada.asp

Art 29 WP (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 1998. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

Art 29 WP (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 of 11 February. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp88_en.pdf

Art 29 WP (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 of 29 January 2004. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf

Art 29 WP (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. Doc. WP 103 of 19 January. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm#wp103

Art 29 WP (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 of 17 August. 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. Last updated: 28 March 2008. 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 16 November 2006. http://www.re-public.gr/en/?p=76

BMG (2007), *Advance Passenger Information Systems*. Retrieved from http://www.businessmobility.org/API/API.html#_Interactive:

Brimmer, E. (2006), "Safeguarding civil liberties in an era of security. A transatlantic challenge". In: Dalgaard-Nielsen, A. and Hamilton, D. S (eds), *Transatlantic Homeland Security. Protecting Society in the Age of Catastrophic Terrorism*. p. 147-171

Cameron, F. (2007), "Transatlantic Relations and Terrorism", in: Spence, D. (ed), *The European Union and Terrorism*. London: John Harper, p.124-142.

CBC (2004), *Indepth: AIR CANADA – History*. Retrieved from http://www.cbc.ca/news/background/aircanada/history.html

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

CBSA (2008), *Advance Passenger Information/Passenger Name Record*. Last updated on 2008-01-16. Retrieved from http://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html

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

CIPPIC (2007), National ID Cards. Last updated 2 June 2007. http://www.cippic.ca/national-id-cards/

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

Deutscher Bundestag (2007), Beschluß zum Bericht des Datenschutzbeauftragten. Drucksache 16/4882 28. 03. 2007. http://dip.bundestag.de/btd/16/048/1604882.pdf

DHS (2006), *Fact Sheet: Secure Borders and Open Doors in the Information Age*. Last updated: 17 January 2006. http://www.dhs.gov/xnews/releases/press_release_0838.shtm

DHS (2006a), *Fact Sheet: Security Improvements to Visa Waiver Program. Last updated*: 30 November 2006. Retrieved from http://www.dhs.gov/xnews/releases/pr_1164919987951.shtm

DHS (2007), *US-VISIT: How It Works.* Retrieved from http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm

DHS-CBP (2004), *UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP)*. 11 May 2004. OJ L 235/15 of 6.7.04.

ECJ (2006), *Judgement of the Court (Grand Chamber) of 30 May 2006 — European Parliament v Council of the European Union*. OJ C 178/1 of 29.7.2006, p. 1. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF

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

EDPS (2005a), Opinion 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). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:218:0006:0010:EN:PDF

EDPS (2007a), *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 of 20 December*. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf

EDPS (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. (2008/C 110/01). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:110:0001:0015:EN:PDF

EPIC (2006), Privacy & Human Rights - An International Survey of Privacy Laws and Developments. Washington D.C.

EPIC (2007), *EU-US Airline Passenger Data Disclosure*. Last updated: November 13, 2007. Retrieved from http://epic.org/privacy/intl/passenger_data.html

EPIC (2007a), *Secure Flight*. Last updated: September 2007. http://epic.org/privacy/airtravel/secureflight.html

EPIC (2007b), *Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved*. August 2007. http://epic.org/privacy/surveillance/spotlight/0807/default.html

EPIC (2007c), Automated Targeting System. Last updated: 27 August 2007. 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

EU Commission (2003), COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE PARLIAMENT. Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach. COM(2003) 826 final of 16.12.2003.

Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0826:FIN:EN:PDF

EU Commission (2005), *COMMISSION STAFF WORKING PAPER ON THE 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*. Doc. (2005) final of 12.12.2005. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/review_2005.pdf

EU Commission (2005a), *Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, Brussels, 24.11.2005. Retrieved from http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf

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

EU Commission (2007), *Passenger Name Record (PNR): FREQUENTLY ASKED QUESTIONS*. Rapid Press release, MEMO/07/294 of 13/07/2007. Retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/294&format=HTML&aged=0&language=EN

EU Commission (2007a), Proposal for a COUNCIL FRAMEWORK DECISION on the use of Passenger Name Record (PNR) for law enforcement purposes. Doc. COM(2007) 654 final of 6.11.2007. Retrieved from http://ec.europa.eu/commission_barroso/frattini/archive/COM(2007)654%20EN.pdf

EU Commission (2008), *EU-US Open Skies: A new era in transatlantic aviation starts on 30 March*, Press release of 28.3.2008, retrieved from

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/474&format=HTML&aged=0&language=EN&guiLanguage=en

EU Commission (2008a), "Communication. Next steps border management". Doc. COM(2008) 69 final, 13.2.08

EU Commission (2008b), *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the next steps in border management in the European Union*. Doc. COM(2008) 69 final of 13 February. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF

EU Commission (2008c), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of […] amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code*. Doc. COM(2008) 101 final of 22/2/2008. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0101:FIN:EN:PDF

EU Council (2001), Regulation (EC) No 539/2001 of 15 March 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. OJ L 81 of 21.3.01, p. 1

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

EU Council (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 andmutual assistance in customs matters to include cooperation on container security and related matters, of 30 March 2004. OJ L 304 30.9.04, p. 32 . http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_304/l_30420040930en00320033.pdf

EurActiv (2007), *EU-US 'Open Skies' agreement*, dossier of 9.10.2007. Retrieved from http://www.euractiv.com/en/transport/eu-us-open-skies-agreement/article-167482

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

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

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

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

EU Parliament and Council (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. 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

EU Parliament and Council (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, p. 72 of 9.4.2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF

FAITC (2003), *Canada's Actions Against Terrorism Since September 11*. Backgrounder of 7 February. Retrieved from http://www.dfait-maeci.gc.ca/anti-terrorism/canadaactions-en.asp

FAITC (2008), *Bilateral Air Negotiations Between Canada and Foreign Countries*. Retrieved from http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/facts-air-eclair.aspx

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

GAO (2004), *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*. Report to Congressional Committees of February 2004. Retrieved from http://www.gao.gov/new.items/d04385.pdf

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

Geyer, F. (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*. CEPS CHALLENGE Paper. 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 of 11 March. Retrieved from http://euobserver.com/9/25809

Goldirova, R. (2008a), *Europeans to face tighter travel rules*. EU Observer of 3 June. Retrieved from http://euobserver.com/24/26260

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

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

Guild, E. (2007), *Inquiry into the EU-US Passenger Name Record Agreement*, CEPS Policy Brief of 22 March. Retrieved from http://shop.ceps.eu/BookDetail.php?item_id=1481

Guild, E. and Brouwer, E. (2006), *The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US*. CEPS Policy Brief of 26 July 2006. 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 Brief No 154 of March 2008. 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: Dalgaard-Nielsen, A. and D. S Hamilton (eds), *Transatlantic Homeland Security. Protecting Society in the Age of Catastrophic Terrorism*. p. 172-196

Hasbrouck, E. (2007), *What's in a Passenger Name Record (PNR)?* Retrieved from http://hasbrouck.org/articles/PNR.html

Helmut, D. (2005), The desert front - EU refugee camps in North Africa? Statewatch news March 2005, 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 of 4 July 2007. Retrieved from http://www.europarl.europa.eu/activities/committees/studies/download.do?file=17239

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

IATA (2007), *IATA history*. Retrieved from http://www.iata.org/about/history

ICAO (1970), *World Air Traffic Growth Rate Slackens in 1970*, News release of 31.12.1970, retrieved from http://www.icao.int/icao/en/nr/1970/pio197017_e.pdf

ICAO (2003), *The Canadian Advance Passenger Information Program*. Doc. FAL/12-WP/38 11/12/03. Retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf

ICAO (2004), *Airline reservation system and passenger name record (PNR) access by states*. Doc. FAL/12-WP/74 of 15/3/04. Retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf

ICAO (2004a), *Advance Passenger Information (API) – a Statement of Principles.* Doc. FAL/12-WP/60 10/3/04. Retrieved from http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp060_en.pdf

ICAO (2008), *Harmonisation of advance passenger information requirements*. Doc. FALP/5-WP/4 of 14/02/08. Retrieved from http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp04_en.pdf

IPC Ontario (2007),

IRRI (2004), "Anywhere But Here: Refugee Processing Centers in Libya", in: *Refugee Rights News, Volume 1 Issue 1*, October 2004. Retrieved from http://www.refugee-rights.org/Newsletters/NorthAfrica/V1N1AnywhereButHere.htm

Joffe, J. (2007), "Wir wollen nur fliegen", in: Die ZEIT, No 34 of 16.8.2007, p.1

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

Koslowski, R. (2006), "Border and Transportation Security in the Transatlantic Relationship", in: Dalgaard-Nielsen, A. and Hamilton, D. S (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 2007. 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", in: The Register of 11 February 2008. Retrieved from http://www.theregister.co.uk/2008/02/11/eu_dhs_eta_spat/

Ludford, S. (2007), "Defending data", ParliamentMagazine of 4 June 2007, p. 15

McClure, G. (2007), How Safe Are Our Ports?, IEEE news, September 2007. Retrieved from http://www.todaysengineer.org/2007/Sep/port-security.asp

Mulder, R. (2005), *The Birth of Air Transport.* Retrieved from http://www.europeanairlines.no/Arcticles_BirthofAirTransport_101004.htm

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

OECD (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Of 23 September 1980. Retrieved from http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html

OPC (2005), *Privacy Protection in a World of Transborder Data Flows.* Doc. Submitted to OECD on 3 October. Retrieved from http://www.privcom.gc.ca/speech/2005/sp-d_051003_e.asp

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

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

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

PI (2007), *Travel Privacy*. Last updated: 18/12/2007. Retrieved from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559086

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

Pospísil, F. (2008), *Czechs became Trojan horses for new US visa waiver programme*. Of 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*. 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. *The Journal of Corporation Law* (Winter):p. 456-477.

Siskin A. (2005), *Visa Waiver Program*. CRS Report for Congress of 19 April 2005. 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: Spence, D. (ed), *The European Union and Terrorism*. London: John Harper, p. 1 - 29

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

Statewatch (2005), US: Report on airline passenger screening. Retrieved from http://www.statewatch.org/news/2005/apr/07us-passenger-screening.htm

Statewatch (2007), *EU: European Commission to propose EU PNR travel surveillance system*. News Online updated 15.7.07. Retrieved from http://www.statewatch.org/news/2007/jul/03eu-pnr.htm

Statewatch (2007a), *EU-US PNR agreement US changes the privacy rules to exemption access to personal data*. News of September 2007. Retrieved from http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm

Statewatch (2007b), *US demands 10 year ban on access to PNR documents*. News of September 2007. 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. Last updated 19 October 2006. http://www.msnbc.msn.com/id/15221111/

TBCS (2005), Canada Border Services Agency. SECTION II - ANALYSIS OF PERFORMANCE BY STRATEGIC OUTCOME. Retrieved from http://www.tbs-sct.gc.ca/rma/dpr1/04-05/BSA-ASF/BSA-ASFd4502_e.asp

Transport Canada (2007), *Canada begins negotiations with European Union on Blue Sky's first anniversary*. Press release No. H 225/07 of 27.11.07 http://www.tc.gc.ca/mediaroom/releases/nat/2007/07-h225e.htm

Transport Canada (2007a), *Passenger Protect Program.* Last updated 2007-10-16. Retrieved from http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm

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

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

Winer, J. (2006), "Cops across borders. The evolution of transatlantic law enforcement and judicial cooperation", in: Dalgaard-Nielsen, A. and D. S. Hamilton (eds), *Transatlantic Homeland Security. Protecting Society in the Age of Catastrophic Terrorism*. London/New York, pp. 106-123

List of legislation

Canada

Aeronautics Act of 1985 (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 of 1970 (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 of 1985 (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 of 2003 (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) of 2001 (2001, c. 27). Retrieved from http://laws.justice.gc.ca/en/I-2.5/

Privacy Act of 1980. 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. Of 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 of 2000 (PIPEDA) (2000, c. 5). Retrieved from http://laws.justice.gc.ca/en/P-8.6/text.html

EU

Charter (2000), CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION of 7 December 2000. OJ C 364 of 18.12.2000, p. 1. Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

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

Agreements

EU – Canada (2005), Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data of 3 October 2005. OJ L82 of 21.3.2006, p.15. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:082:0015:0019:EN:PDF

Related documents:

EU Commission (2005b), *Decision on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada*

Border Services Agency. Decision of 6 September. OJ L 91, p. 49. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:0060:EN:PDF

CBSA (2005a), *COMMITMENTS BY THE CANADA BORDER SERVICE AGENCY IN RELATION TO THE APPLICATION OF ITS PNR PROGRAM.*

OJ L 91, p. 53. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:0060:EN:PDF

EU – US (2004), Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. OJ L 183 of 20.5.2004, p. 84. Retrieved from http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf

CBP (2004), UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION. Of 11 May 2004. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:EN:HTML

EU Commission (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

EU – US (2006), (Interim) 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. Of 16 October 2006. OJ L 183 of 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 on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) of 23/26 July 2007. OJ L 204 of 4.8.2007, p. 18. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:EN:HTML

DHS letter (2007), Letter from Michael Chertoff, Secretary of Homeland Security, to Mr Luis Amado, President of the Council of the European Union. Without date. OJ L 204 of 4.8.2007, p. 21. 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. Without date. OJ L 204 of 4.8.2007, p. 25. 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 REGARDING THE UNITED STATES VISA WAIVER PROGRAM AND RELATED ENHANCED SECURITY MEASURES. Of 26 February. Retrieved from http://www.vlada.cz/scripts/detail.php?id=31921

List of Abbreviations

ACLU	American Civil Liberties Union
API	Advance Passenger Information
APIS	Advance Passenger Information System
APP	Advance Passenger Processing
APP	APIS Quick Query (US CBP)
Art 29 WP	Data Protection Working Party under Article 29 of Directive 95/46/EC
BMG	Business Mobility Group
CAPPS	Computer Assisted Passenger Prescreening System (US)
CBC	Canadian Broadcasting Corporation
CBP	US Customs and Border Protection
CBSA	Canadian Border Services Agency
CCRA	Canada Customs and Revenue Agency (now CBSA)
CIC	Citizenship and Immigration Canada (Agency)
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CRS	Computer Reservation System
DCS	Departure Control System
DHS	US Department of Homeland Security
DP	Data protection
DPA	Data protection authority
ECJ	European Court of Justice
ECHR	European Convention on Human Rights and Fundamental Freedoms
EDPS	European Data Protection Supervisor
EPIC	Electronic Privacy Information Center
ESTA	Electronic System of Travel Authorisation (EU)
FAA	Federal Aviation Administration
FAITC	(Ministry of) Foreign Affairs and International Trade Canada
FOIA	Freedom of Information Act US 1966
GAO	US General Accounting Office
GDS	Global Distribution Systems
ICAO	International Civil Aviation Organisation
IRPA	Immigration and Refugee Protection Act (Canada)
IRRI	International Refugee Rights Initiative

MRZ	Machine readable zone (of a passport)
NRAC	National Risk Assessment Centre (CBSA)
OPC	Office of the Privacy Commissioner of Canada
OSI	Other Service Information
p.	page
PAU	local Passenger Analysis Unit (CBSA)
PAXIS	Passenger Information System (of CBSA)
PI	Privacy International
PIPEDA	Personal Information Protection and Electronic Documents Act, Canada 2000
PNR	Passenger Name Record
PTU	(regional) Passenger Targeting Unit (CBSA)
RFID	Radio frequency identification
s.	section
SF	Secure Flight
SSR	Special Service Request
TBCS	Treasury Board of Canada Secretariat
TSA	Transportation Security Administration (US)
WP	Working Party

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

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 itinerary 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
16. Seat number	16. Split/Divided PNR information	16. Seat information, including seat number

17. Date of ticket issuance	17. Email 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 travelers on PNR	
	31. Seat information	
	32. One-way tickets	
	33. Any collected APIS information	
	34. ATFQ fields	

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