Border Controls, Surveillance and Counter Terrorism

Elspeth Guild
BORDER CONTROLS, SURVEILLANCE AND COUNTER TERRORISM

1. Introduction

One of the most commonly repeated statements regarding international law on border controls and migration is that of the European Court of Human Rights: ‘The Court reiterates that Contracting States have the right as a matter of well-established international law and subject to their treaty obligations, including the Convention, to control the entry, residence and expulsion of aliens’.\(^1\) The extent of the right to control entry and the limits which may be placed on that right is the subject which I examine here. In the jurisprudence of the European Court of Human Rights and elsewhere, the limits of state action in respect of border controls on persons is limited by the human rights obligations which states have ratified. This means that when examining states’ border control activities, the human right to seek asylum, non-refoulement and the right to respect for private and family life are the points of departure against which states’ practices and law are tested. States are rarely required to justify the reasons for their border control laws and practices beyond the human rights limits. Where they are, the answer is usually one of state sovereignty which permits the exercise of border controls in the interests of national security (though there are others perspectives).\(^2\) Until recently this claim to national security was accepted with little investigation. Recent case law from the Court of Justice of the European Union (on the proposed EU-Canada PNR Agreement) and the US courts (on the Executive Order No 13780 and its predecessors barring from entry to the USA nationals of certain countries) appear to be changing this status quo. The working paper sets out the issue of border control and personal data collection in pursuit of counter-terrorism objectives, the challenges which are presented for the right to privacy and the recent developments in the form of the CJEU’s Opinion on the proposed EU Canada PNR Agreement\(^3\) and very briefly, the challenge of the US 9th Circuit Appeal Court to the claim of the US Government in defence of its executive order protecting the nation from foreign terrorist entry into the United States that national security trumps all other constitutional claims.

---

\(^1\) D. v. the United Kingdom. 2 May 1997, Reports of Judgments and Decisions 1997-III.
\(^3\) EU:C:2017:592.
2. **Who is coming to your country?**

Interest in knowing who the foreigners are who are arriving at national borders has been a matter of substantial interest to many countries, not least in Europe and the USA. While visa requirements provide a tool to ensure that all nationals of some countries must undergo a pre-travel clearance check (in the form of a visa application and determination), many states have not been satisfied with this tool. Some, like the USA, have introduced advanced authorisation systems for all foreign traveller to their country (the Electronic System from Travel Authorization, ESTA). The EU is currently considering legislating for a similar system. These systems provide advanced information about all foreign travellers and as has become apparent with the endless addition of questions to ESTA application forms, can be quick flexible.

To be successful, these systems must be accompanied by carrier sanctions which penalise transport companies for transporting passengers without visas or other prior authorisation.

But these information sources, visas, ESTAs etc, do not provide a full picture of all passengers travelling to a country. They are limited to foreigners. Many countries wish to have complete information about all arriving passengers, including their own nationals who are returning. This information is available from the airlines in a number of forms, first: advance passenger information (API). This is information from carriers records about all passengers on each flight, train or ship which is sent to the destination country within specified periods before departure. According to the International Air Transport Association (IATA) 39 countries require airlines to send API before a flights arrival. The USA first required this data to be provided by legislation in 1991. Other states followed suit. A further 32 countries are planning to introduce this requirement. API consists of the information held in the machine readable zone of passports and details of the travel. IATA is seeking that all countries which demand API information harmonise their require-

---

5 API data required for instance under EU Directive 2004/82 requires only: the number and type of travel document used; nationality; full names; date of birth; border crossing point of entry; code of transport; departure and arrival time of the transportation; total number of passengers carried on the transport; initial point of embarkation.
6 49 U.S. Code § 44909 — Passenger manifests.
ments to ‘international standards and guidelines.’ This indicates that there is not or at least not yet a harmonised norm. API was given a specific international status by Security Council Resolution 2178 of 24 September 2014 which calls on all states to counter and prevent the movement of terrorist foreign fighters⁸ including by providing advance passenger information to countries which request this.⁹

A number of countries, however, have not been satisfied with this source of information about who is coming to their borders. These countries created obligations on travel companies and airlines to make available to them another source of information created by the private sector to simplify commercial activities of travel related businesses: passenger name records (PNR). PNR files are an industry wide customer information system, created and stored on all passengers who contract with transport (and other) companies. This data includes both foreigners and citizens, a distinction which is of only marginal interest to travel companies but of great importance to states. According to IATA, six countries currently require PNR data to be made available to them on all passengers travelling to their country and a further 30 countries are developing or considering implementing such a requirement.¹⁰

3. **Passenger Name Records**

Passenger name records (PNR) are files created by carriers (normally airlines, train, bus and shipping companies) regarding all passengers whom they carry which contain all information necessary for the processing and control of reservations. PNR data includes a much wider range of data than API. It includes information such as the name of the passenger, travel dates, itineraries, seats, meal preferences, fidelity cards, all passengers booking together, spe-

---

⁸ Paragraph 2: ‘that all States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting…’, Security Council Resolution 2178 of 24 September 2014

⁹ Paragraph 9 ‘Calls upon Member States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee established pursuant to resolutions 1267 (1999)and 1989 (2011) (“the Committee”), and further calls upon Member States to report any such departure from their territories, or such attempted entry into or transit through their territories, of such individuals to the Committee, as well as sharing this information with the State of residence or nationality, as appropriate and in accordance with domestic law and international obligations;’ Security Council Resolution 2178 of 24 September 2014

cial requirements such as wheelchairs, baggage, contact details, addresses, phone numbers including mobile numbers and means of payment. As such PNR data is much more sensitive than its API counterpart as it contains information which is much more intrusive into the lives of the individuals who provide it. From special needs, information about health can be deduced. From information about meal preferences (such as Halal) assumptions about religion can be made. From payment methods, relationships with third parties, such as companies paying for travel of passengers can be discovered.

As some states have become increasing concerned about the possible convergence of border crossing and terrorism risks (in particular after the attacks in the USA on 11 September 2001), interior ministries led by the US Department of Homeland Security sought ways to obtain ever more accurate and detailed information about passengers. PNR became of interest to state authorities. Generally, states’ collection and use of vast amounts of personal data as a solution to the risk of terrorism intensified after 2001 to the point where the US whistleblower, Edward Snowden, revealed an astonishing network of public and private tools used by US (and other) intelligence services to collect electronic data in bulk.\textsuperscript{11} The border as a data collection site where people are relatively vulnerable – not yet admitted to a state (even if it is their own) – and so in a grey zone regarding constitutional protections\textsuperscript{12} became interesting to some state authorities in the pursuit of counter terrorism objectives.\textsuperscript{13} What was the advantage, in that framework of PNR data?

While API contains information which states have placed in their citizens’ passports and the individual’s travel itinerary as known by the travel company, PNR files are more extensive. They are created on the basis of the contract between the individual and the travel company and sensitive both as to the elements of the private life of the individual and as regards commercially sensitive information for the company. Travel companies were unwilling to provide this information to state authorities without specific legislation requiring them to do so. The first country to so legislate was the USA in 2002.\textsuperscript{14}

\textsuperscript{11} Bauman, Zygmunt, et al. ‘After Snowden: Rethinking the impact of surveillance.’ \textit{International political sociology} 8.2 (2014): 121-144.

\textsuperscript{12} Neuman, Gerald L. \textit{Strangers to the constitution: Immigrants, borders, and fundamental law}. Princeton University Press, 2010.

\textsuperscript{13} Guild, Elspeth, ‘Who is Sharing Personal Data Obtained in Immigration Procedures with Whom?’ Immigration Law Practitioners Association European Update, September 2014.

\textsuperscript{14} The Federal Register/Vol. 67, No. 122/Tuesday, June 25, 2002/Rules and Regulations permits the sharing of this data.
terrorism and serious crime.\textsuperscript{15} However, many were critical about the compatibility of the right to privacy with the sharing PNR files (which result from information which customers provide to a private company) with state authorities. The privacy issue became explicit fairly quickly following the adoption of the US legislation as travel companies subject to the jurisdiction of EU states found themselves between a rock and a hard place.\textsuperscript{16} Either they flouted US legislation and refused to provide PNR data to the US or they provide it and breach EU privacy law.

Thus the need for PNR agreements arises from privacy protection legislation in many countries, such as the Member States of the European Union.\textsuperscript{17} By 2003 discussions were taking place between the EU and the USA on PNR transfers from the EU to the USA which resulted in the first EU-US PNR Agreement in 2004.\textsuperscript{18}

In fact, most airlines do not host their own databases for PNR. Instead they store PNR in a Computerized Reservation System (or Global Distribution Systems) which are operated by three companies – Amadeus (registered in Spain), SABRE (listed on the US NASDAC exchange) and Travelport (which is comprised of Galileo and Worldspan and listed on the NY Stock Exchange as a US company). Because PNR is a tool of the travel industry, it links data on customers such as hotel bookings, car hire etc but also information useful to staff such as comments on customers.\textsuperscript{19}

4. The EU and PNR Agreements with third countries

The EU has been active in the field of transfer of PNR data. The first agreement with the USA in 2004 was followed by a second agreement with Canada in 2006 and an agreement with Australia in 2008. All these agreements were time limited. None has been uncontroversial. Each agreement requires the European Commission to issue an adequacy decision regarding the complementarity of the agreement with the EU’s data protection regime contained


in (the then applicable) Directive 95/46. Each time there has been concern and opposition regarding the (lack of adequate) protection of EU citizens’ privacy provided by the non EU party concerning the use of the data. This resistance has come in the form of negative opinions from the EU’s Article 29 Working Party (established under the Directive and composed of a representative of the data protection authority of each Member State, the European Data Protection Supervisor (EDPS) and the Commission), annulment actions by the European Parliament before the Court of Justice of the European Union and civil society.

Revelations about the US National Security Agency’s (NSA) mass surveillance programmes by Edward Snowden in 2013 generated substantial concern in the field of privacy protection. Nowhere was this more pronounced than in the EU. A series of judgments by the CJEU in respect of privacy protection has left a number of EU agreements with third countries regarding data sharing in doubt.

What is particularly interesting of PNR agreements is that states undertake to allow the transmission of personal data of people (the majority of whom are likely to be their citizens) to another country for the purposes of fighting terrorism and serious transnational crime. The personal data includes a wide range of elements, has been collected by the private sector on the basis of the contractual arrangements which each business in the sector agrees with the customer and are covered by consumer protection rights. In the EU such personal data is protected by Directive 95/46 which is in the process of being replaced by a much more onerous set of rules protecting privacy and personal data under the General Data Protection Regulation (GDPR) which must be in effect in the 28 Member States by 25 May 2018.

The GDPR tightens up controls and obligations on the private sector in respect of the collection, use, transmission (or other sharing) and deletion of personal data and includes the so-called ‘right to be forgotten’. For the public sector, the Data Protection Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for

the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data applies.²⁵

According to the Commission the Directive for the police and criminal justice sector ensures that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action.²⁶ At the same time more harmonised laws also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe. It also places very strict limitations on the circumstances under which personal data can be shared with a third country (a country outside the EU) for the purposes of law enforcement (including of course the fight against terrorism and serious transnational crime).²⁷ As this is a directive, it must be transposed by the 28 Member States by 6 May 2018. Thus the PNR agreements must be accompanied by a Commission decision that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Because these adequacy decisions of the Commission are based on the Commission’s appreciation of the situation in the third country they can be challenged before the CJEU (or the general court).

²⁷ Preamble 64 of the Directive 2016/680 gives the rationale ‘Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.’
5. **EU-Canada PNR Agreement**

In 2006 the EU concluded its first passenger name record agreement with Canada. The Agreement expired in September 2009. In 2010 the EU commenced negotiations for new PNR agreements with the Australia, Canada and the USA. While the agreements with Australia and the US were concluded in 2012, the EU-Canada agreement was only initialled on 6 May 2013 with the proposal for a Council decision adopting the agreement in July 2013. However, on 6 June 2013 the first of the Snowden revelations about the NSA’s mass surveillance programme appeared in the Guardian newspaper.\(^{28}\)

First the EDPS issued a negative opinion, then the Council accepted that the European Parliament had to approve the decision to conclude the agreement. Although the Council went ahead and signed the agreement in June 2014 only seeking the Parliament’s approval on 7 July 2014, the Parliament was unhappy with the data protection arrangements and sought the opinion of the CJEU on 25 November 2014 which was duly handed down on 26 July 2017.\(^{29}\)

6. **The Judgment in a Nutshell**

The CJEU held that the agreement could not be concluded in its (then) current form because several of its provisions were incompatible with fundamental rights recognised by the EU. As the proposed agreement would permit the systematic and continuous transfer of PNR data on all air passengers to the Canadian authorities, use, retention for five years and possible transfer to other authorities and to other non EU countries, the CJEU concluded that it entailed an interference with the EU fundamental right to respect for private life. It also entailed an interference with the EU fundamental right to personal data protection. Because there is an interference with two EU fundamental rights it must be justified by the pursuit of an objective of general interest to be lawful. Further, to be justified the interference must be strictly necessary and lay down clear and precise rules. As regards sensitive data (covering racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning a person’s health or sex life) the agreement is inadequate regarding their protection. As regards all other PNR data, the objective of identifying risk to public security presented by persons not known to the relevant services justifies automated analysis of PNR data for the purposes of border control. Once admitted to Canada, the use of PNR data must be subject to different (and presumably more stringent) rules.

---


which include an a priori review to be carried out by a court or other independent administrative authority of the necessity of access to the PNR data for the purposes of prevention, detection or prosecution of crime. After departure from Canada, continued storage is no longer strictly necessary in respect of passengers in respect of whom no risk has been identified as regards terrorism or serious transnational crime. For those passengers where a risk has been identified, then retention and storage for up to five years is permissible but subject to the same stringent requirements as regards access as apply when the passenger is in Canada.

The CJEU provides a list of six requirements which the agreement must include to fulfil EU data protection obligations (see Annex 1).

7. **Adjudicating Necessity in Preventing, Combating, Repressing and Eliminating Terrorism**

When is an interference with the right to respect for privacy and data protection permissible on the basis of preventing, combating, repressing and eliminating terrorism through the use of border controls? This is the question which the CJEU is required to answer.

The objective and justification for the PNR agreement, according to its preamble, is to prevent, combat, repress, and eliminate terrorism and terrorist-related offences as well as other serious transnational crime. The agreement sets out the definition of terrorism and terrorist related crimes as well as serious transnational crime. Article 5 of the agreement confirms that the Canadian Competent Authority is deemed to provide an adequate level of protection for the processing and use of PNR data consistent with EU standards.

But is it necessary to transfer PNR data for this purpose? The CJEU notes that the Commission and the Council have no precise statistics on the basis of which to ascertain the contribution which PNR data makes to the prevention and detection of crime or terrorism or its investigation. However, the CJEU notes that third countries and Member States which already use PNR data for law enforcement purposes claim that it is essential. The EU proposal (now adopted) for an intra EU PNR transfer system states that experience of certain countries (unspecified) shows that the use of PNR data has led to critical progress in the fight against drug trafficking, human trafficking and terrorism and a better understanding of the composition and operations of terrorist and other criminal networks. This statement is unchallenged by the CJEU.

---

30 Paragraph 55 of the judgment.
32 Paragraph 55 of the judgment.
The Canadian authorities, according to the CJEU have done better in producing some statistics. 28 million air passengers flew between the EU and Canada between April 2014 and March 2015. According to the Canadian authorities PNR data on those passengers made it possible to arrest 178 people (though it is not clear on what grounds).\textsuperscript{33} 71 drugs seizures were made, 2 child pornography cases were identified, and in 169 cases PNR made it possible to initiate or further pursue investigations in relation to terrorism.\textsuperscript{34} No statistics on trials or convictions were provided.

As regards the purpose and content of the agreement, the CJEU found that there were two objectives, first the prevention etc of terrorism and terrorist related offences and other serious transnational crime and secondly the respect for fundamental rights in particular the right to respect for private life and the right to the protection of personal data.\textsuperscript{35} Yet, the transfer of PNR data to Canada and its use there is only justified by the objective of ensuring public security there. Thus such transfer is only lawful if there are rules in Canada which guarantee a level of protection which is essentially equivalent to that guaranteed in the EU.\textsuperscript{36}

As the CJEU found that transfer of PNR data, its use and its subsequent transfer to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or the authorities of third countries constitute interferences with the right to respect for privacy (Article 7 EU Charter of Fundamental Rights)\textsuperscript{37} it must be justified. The justification must be consistent with the principle of proportionality and strictly necessary to achieve the objective.\textsuperscript{38} The processing of personal data cannot be justified on the basis of the consent of the passenger as the passenger provided his or her information for reservation purposes (not for transmission to third parties).\textsuperscript{39} Presumably this would be the case irrespective of the wording of any consent box which the airline required to be ticked before completing the reservation. The tendency of companies to require consent for use of personal data

\textsuperscript{33} This rather startling fact which is inherently related to the proportionality of the agreement is repeated at paragraph 152 of the judgment but the CJEU chose not to attack the agreement on the ground that there is no proportionality between the number of persons whose personal data is shared on a systematic and untargeted manner and the extremely low number of useful outcomes for the state using the data.

\textsuperscript{34} Paragraph 56 of the judgment.

\textsuperscript{35} Paragraphs 81 and 84 of the judgment.

\textsuperscript{36} Paragraph 93 of the judgment.

\textsuperscript{37} Paragraph 125 of the judgment.

\textsuperscript{38} Paragraph 140 of the judgment.

\textsuperscript{39} Paragraph 143 of the judgment.
of those using their services for purposes far beyond what the consumer expected has been subject of critical judicial consideration.\textsuperscript{40}

Yet, the objective of fighting terrorism and serious transnational crime is a general interest of the EU.\textsuperscript{41} The transfer of PNR data is appropriate for the purpose of ensuring public security and largely facilitates and expedites security and border control checks. However, there are a number of limits. First, there must be a sufficiently clear and precise definition of the PNR data which can be transferred. Mere reference to PNR data as including available frequent flyer and benefit information (free tickets, upgrades, etc) is inadequate in this regard. The CJEU was particularly unimpressed by the use of ‘etc’.\textsuperscript{42} The use of the terms ‘all available contact information’ and ‘all available payment/billing information’ are similarly inadequate for lack of precision and clarity in the view of the CJEU. This is also the case regarding the reference to ‘all supplementary information’.

Sensitive data, which includes any information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership a person’s health or sex life, (as defined in the agreement itself) while not directly solicited in PNR data may be included in it. The examples which are usually put forward relate to choice of meals (Halal, vegetarian, Kosher etc) which could be taken as proxies for religious or philosophical beliefs. These characteristics, in the absence of regard to the personal conduct of the traveller, if processed for the purposes of combating terrorism and serious transnational crime would breach EU guarantees in respect of privacy and data protection.\textsuperscript{43} This sensitive data can only be transferred to Canada if there are precise and particularly solid justifications.

The agreement acknowledges that the Canadian authorities will submit the systematically collected data which is not targeted in any way to automated processing based on pre-established models and criteria and cross-checking with various databases.\textsuperscript{44} The objective is a risk assessment for the purpose of public security (that of Canada not the EU) which automated processing is carried out on the basis of unverified personal data necessarily presenting the possibility of a margin of error. This is a point which the EDPS had stressed in his opinion on the agreement suggesting that evidence indicates that the margin of error appears to be significant. The CJEU rightly focuses on how the pre-established models and criteria are created. In particu-

\textsuperscript{41}Paragraph 149 of the judgment.
\textsuperscript{42}Paragraph 156 of the judgment.
\textsuperscript{43}Paragraph 165 of the judgment.
\textsuperscript{44}Paragraph 168 et seq of the judgment.
lar as the algorithms which result from these models and criteria must be based on something, the concern is whether those criteria are discriminatory on prohibited grounds such as race, religion, nationality, membership of a social group, political or philosophical opinion, sexual orientation etc. The obligation to ensure that the models and criteria result in only those in respect of whom there is a reasonable suspicion of participation in terrorism or serious transnational crime is paramount. Further as far as cross checking with other databases – those databases must also be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime. It is worth noting that in a study undertaken in four Member States in 2005 — 2007 on the accuracy of information on third country nationals submitted by the authorities to the Schengen Information System, according to checks by national data protection authorities up to 40% was either inaccurate or unlawfully stored.\(^{45}\) One can only hope that the Canadian databases are more accurate and in conformity with the relevant law.

The CJEU insisted on a further requirement (specified in the agreement) that in respect of automated processing of personal data, where a positive result occurs there must be an individual re-examination by non-automated means before an individual measure adversely affecting air passengers is adopted.\(^ {46}\)

The CJEU found that the automated processing of personal data facilitates and expedites security checks, in particular at borders.\(^ {47}\) It is aimed at identifying persons who are not, at that stage, known to the competent authorities and who may potentially present a risk and therefore may be subject to further examination. The court accepted that the exclusion of certain categories of persons or certain areas of origin from the automated processing would be liable to prevent the achievement of the objective which is to identify through verification of the data, persons liable to present a public security risk. Thus the inclusion of all PNR data without targeting was accepted. However, as the data processing is for the purposes of border checks on unknown risks, once a person has crossed the border the objective has been exhausted. The use of data after the passenger has entered Canada must be based on new circumstances justifying that use. There must be objective criteria in order to define the circumstances and conditions under which the authorities are authorised to use the data. This must include an a priori review by a court or independent administrative body following a rea-


\(^ {46}\) Paragraph 173 of the judgment.

\(^ {47}\) Paragraph 187 of the judgment.
soned request by the competent authorities to access the data. The objective must also be limited to the prevention, detection or prosecution of crime.\textsuperscript{48}

After departure from Canada the objective of the data processing is finished at least in respect of persons who were never identified as a security risk. Indeed even in respect of those who were identified, the CJEU notes that both the Council and the Commission consider that ‘the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks, do not justify the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime.’\textsuperscript{49} However, in specific cases where there is objective evidence that the passenger may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada their specific data can be stored for up to five years.\textsuperscript{50} But the data must always be held in Canada and at the end of the retention period all data must be irreversibly destroyed.

As regards disclosure of PNR data to third countries, the same rules and protections must apply as regards its use in Canada (dealing with the US NSA issue). Just to make the matter completely clear the CJEU stated that disclosure to a third country requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under the relevant EU directive finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred.\textsuperscript{51}

While the Opinion does not exclude the bulk collection of data, a disappointment to privacy advocates in Europe, it does place very substantial limits on the use and deletion of data.\textsuperscript{52} It is a very substantial privacy protective decision regarding how personal data can be used where the collection is justified on the grounds of action against terrorism.

\textsuperscript{48} Paragraphs 196 et seq of the judgment.
\textsuperscript{49} Paragraph 205 of the judgment.
\textsuperscript{50} Paragraphs 207 and 209 of the judgment.
\textsuperscript{51} Paragraph 214 of the judgment.
8. The US Executive Orders ‘Protecting the Nation from Foreign Terrorist Entry into the USA’

So far in 2017, the US Government, has issued three executive orders, the most recent on 24 September 2017, banning nationals from some countries from entering the USA. The objective of the orders is stated to be national security and in particular counter-terrorism. The first two bans — Executive Orders of 27 January 2017 and 6 March 2017 — focused on nationals of Iran, Iraq, Libya, Somalia, Sudan, Syria and Yemen (Iraq was taken off the list in March). The Executive Orders have been partially stopped by various Circuit Courts (mainly the Hawaii Court, the 4th and 9th Circuits and the Supreme Court) and the matter has gone to the Supreme Court for a full hearing (eventually). The three travel bans have the same vocation: to require all states to provide information regarding their citizens (and those foreigners about whom they hold information) to the US authorities in return for being left off the banned list. The most recent Travel Ban sets out for the first time the information which states must provide about their citizens with a three fold objective – (a) to confirm the identity of people seeking to enter the USA; (b) identification of persons applying for any other benefit under US immigration laws and (c) assessment of security or public safety threats. The baseline contains three categories of information:
(a) identity-management information;
(b) national security and public safety information;
(c) national security and public safety risk assessment.

Further specificity is provided in the Travel Ban as follows:

Identity management information: states must provide to the US authorities information needed by the US to determine whether individuals seeking to go or stay in the USA are who they claim to be. This focuses on integrity of documents. The criteria are whether the country issues electronic passports embedded with data to enable confirmation of identity; reports lost or stolen passports to appropriate entities (unspecified); and makes available on (US) request identity-related information not included in its passports. This extra information is not defined or limited.

National security and public safety information: the US Government expects foreign governments to provide information about whether persons (seeking to go to the US) pose a national security or public-safety risk (not limited to the USA). The criteria are whether the country makes available known or suspected terrorist and criminal history information upon request; whether the country provides passport and national identity document exemplars; whether the country impedes the US Government’s receipt of information about passengers and crew traveling to the USA (this is a reference
to Passenger Name Records held by airlines). This category might cover new Regulation 2017/458 on databases and EU external frontiers to catch EU national ‘foreign’ fighters.

**National security and public safety risk assessment**: this category focuses on national security risk indicators. The criteria are: whether the country is a known or potential terrorist safe haven; whether it is a participant in the Visa Waiver Program; whether it regularly fails to receive its nationals subject to final orders of removal from the USA.

The US authorities’ stated objective is the collection of personal data from states in pursuit of national security (in particular counter-terrorism) objectives of the US. Particularly in the first Executive Order, the counter-terrorism objective was stated without any apparent justification that the states listed in the banning order and their citizens are specifically linked with a terrorism threat to the USA. This issue was raised before the US court and while the litigation is far from finished, the US 9th Circuit Appeals Court has challenged the US government’s claim that national security (and counter-terrorism as part of it) is an overriding interest which trumps all other claims.


Normally, US courts have been reluctant to challenge claims by the executive that measures are required on the grounds of national security. However, the executive orders banning nationals of certain states from entry into the US has caused the 9th Circuit Appeals Court in particular to question this assumption. The court considered the US Government’s argument that its national security claim should not be subject to judicial consideration. The court held that ‘the Government’s rote invocation of harm to ‘national security interests’ as the silver bullet that defeats all other asserted injuries’ is not convincing (page 74). Relying on previous authority, it held that with national security may be the most compelling of government interest it does not mean that it will always tip the balance of equities in favour of the government. The court’s obligation to uphold the constitution means that it must examine whether the state’s claim of harm to national security still outweighs the competing claim of injury. The court found in favour of the competing claim of injury on the basis of a claim grounds in the US constitution (to natural and legal persons in the USA). The willingness of the court to examine and reject the states justification of action at the border on the grounds of counter-

---

terrorism (national security) is the aspect of interest here. The reasoning based on the US constitutional right of people to enjoy the presence of foreigners close to them is quite different from that of the CJEU (privacy and data protection). But in both cases the claims of counter-terrorism and national security have been questioned, examined and found insufficient.

10. Conclusions

Border controls provide particular opportunities for states to collect vast amounts of data about people travelling. The justification for the collection of personal data in the context of border controls used in the EU and the USA has been national security in particular in the form of counter-terrorism. The measures taken include requiring the private sector travel industry to divulge all the personal data they hold on passengers they carry across borders and requiring state authorities to provide all information including suspicions they have about their own citizens in the context of counter-terrorism.

In both cases courts in the EU and the USA have begun to ask questions about the legitimacy of these personal data collection projects. While the grounds have been very different the outcomes challenge the state authorities claims that counter-terrorism is (using the words of the US 9th Circuit Appeals Court) a silver bullet which outweighs all other considerations.
IX. Answer to the request for an Opinion

In the light of all the foregoing considerations, it must be held that:
...
(3) the envisaged agreement must, in order to be compatible with Articles 7 and 8 and Article 52(1) of the Charter:
   (a) determine in a clear and precise manner the PNR data to be transferred from the European Union to Canada;
   (b) provide that the models and criteria used in the context of automated processing of PNR data will be specific and reliable and non-discriminatory; provide that the databases used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;
   (c) save in the context of verifications in relation to the pre-established models and criteria on which automated processing of PNR data is based, make the use of that data by the Canadian Competent Authority during the air passengers’ stay in Canada and after their departure from that country, and any disclosure of that data to other authorities, subject to substantive and procedural conditions based on objective criteria; make that use and that disclosure, except in cases of validly established urgency, subject to a prior review carried out either by a court or by an independent administrative body, the decision of that court or body authorising the use being made following a reasoned request by those authorities, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime;
   (d) limit the retention of PNR data after the air passengers’ departure to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime;
   (e) make the disclosure of PNR data by the Canadian Competent Authority to the government authorities of a third country subject to the condition that there be either an agreement between the European Union and that third country equivalent to the envisaged agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, covering the authorities to which it is intended that PNR data be disclosed;
   (f) provide for a right to individual notification for air passengers in the event of use of PNR data concerning them during their stay in Canada and after their departure from that country, and in the event of dis-
closure of that data by the Canadian Competent Authority to other authorities or to individuals; and

(g) guarantee that the oversight of the rules laid down in the envisaged agreement relating to the protection of air passengers with regard to the processing of PNR data concerning them will be carried out by an independent supervisory authority.