Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber?

Arthur Rizer
DOG FIGHT: DID THE INTERNATIONAL BATTLE OVER AIRLINE PASSENGER NAME RECORDS ENABLE THE CHRISTMAS-DAY BOMBER?

Arthur Rizer

I. CONFLICTING PHILOSOPHIES ON PRIVACY: UNITED STATES V. EUROPEAN UNION

II. HISTORY OF THE LEGAL CONFLICT ...........................................................79
   A. September 11, 2001: Everything Changes ........................................83
   B. November 11, 2001: The Aviation and Transportation Security Act ..............................83
   C. May 28, 2004: Agreement to Transfer ........................................85
   D. May 30, 2006: The European Court of Justice Rejects the Agreement .......86
   E. July 23, 2007: A New Agreement Is Reached........................................88

III. BALANCING COUNTERVAILING POSITIONS ................................. 91
   A. New Challenges .................................................. 92
   B. New Laws? ................................................. 96
   C. Balancing Security of Data with Security of a Nation ................. 99

IV. CONCLUSION ................................................ 104

Almost immediately after the terrorist attacks on September 11, 2001, the United States and the European Union (EU) started a battle over Passenger Name Records (PNR).1 After the attacks, the United States began to assign risk-assessment ratings to all travelers entering and exiting the country.2 As part of this risk assessment, the United States gathered passenger information, in the form of PNRs, from airline records.3 This information was shared among domestic and international law-enforcement agencies as part of a data-sharing agreement.4 Despite an ostensible motivation to collaborate on the

---

3. Id.
4. Id. at 551–52.
agreement, “the United States and the European Union have struggled to find common legal justification for PNR transfers.” 5 Specifically, after the European Court of Justice (ECJ) struck the data-sharing agreement between the European Union and the United States, a small legal-war regarding the use and sharing of PNRs erupted between data-privacy advocates and national-security promoters who believe security interests trump privacy concerns. 6

On December 25, 2009, amid this data-sharing conflict, Umar Farouk Abdul Mutallab attempted to detonate plastic explosives that were concealed in his underwear while on an airplane. 7 Mutallab travelled freely to Amsterdam from Nigeria and then to Detroit aboard Northwest Airlines Flight 253. 8 This failed attack sheds new light on the discussion of PNR-sharing and raises the question of whether the limitations on PNR-sharing enabled an attack like this to happen. Indeed, the December 25th attempted attack “is a vivid reminder that terrorists will stop at nothing to kill Americans.” 9 And, as Valerie Caproni, General Counsel to the Federal Bureau of Investigation (FBI) stated, “the attempted bombing on December 25th was a failure to connect dots that probably could have been connected.” 10

This Article will explore the legal history of PNR-sharing starting from September 11, 2001 to the signing of the new sharing agreement dated July 23, 2007. In addition, this Article will discuss the roots of the PNR conflict, focusing on the conflicting approaches the United States and the European Union take regarding privacy issues and how these approaches led to the discord over PNRs. Discovering the roots of this conflict is particularly important in order for the two governments to avoid future tension.

This Article will also survey the upcoming challenges to the current agreement and the new PNR laws on the horizon, 11 and address how the Lisbon Treaty may affect this issue. Last, this Article will scrutinize the new agreement between the United States and the European Union, specifically

5. Id. at 552.
6. See infra Part III.B–C.
10. Audio Recording: Valerie E. Caproni, Gen. Counsel, Fed. Bureau of Investigation, Address at the ABA 5th Annual Homeland Security Law Institute Conference (Mar. 4, 2010) (on file with the ABA Section of Administrative Law and Regulatory Practice). Ms. Caproni also stated that the dots could have been connected “with the benefit of hindsight 20/20.” Id.
questioning if the agreement properly balances personal-data security with national-security concerns or whether it allows for more situations like Umar Farouk Abdul Mutallab's in the name of privacy.

I. CONFLICTING PHILOSOPHIES ON PRIVACY: UNITED STATES V. EUROPEAN UNION

The protection of privacy rights is a global issue faced by all nations. The drama that played out between the United States and the European Union over PNR-data transfers is a prominent example of the clash between conflicting philosophies on privacy protection.

The tension between the United States and Europe stems from the essence of how the two sovereigns perceive the issue of privacy protection. Both the United States and the European Union view privacy as a fundamental right, yet their approaches to protecting this right differ significantly. One U.S. official


13. See Salbu, supra note 12, at 665. There is a "difference in attitude between the EU and the US surrounding the area of protection of rights and civil liberties, extra caution is needed when concluding agreements that allow for the personal data of EU citizens to be transferred from the EU to the US." SHARON NOLAN, CTR. OF EUR. STUDIES, UNIV. OF LIMERICK, EU SECURITY VERSUS CIVIL LIBERTIES: THE CASE OF PNR DATA TRANSFER 2 (2006) (on file with author).

14. Carter Manny, EU Privacy and U.S. Security: The Tension between EU Data Protection Law and U.S. Efforts to Use Airline Passenger Data to Fight Terrorism and Other Crimes I (undated) (unpublished manuscript) (on file with author). Europe's view is that privacy "laws reflect the view that privacy is a fundamental human right which governments are obligated to protect. This protection applies not only to use of the data within Europe, but to international transfers to countries outside the EU." Id. The United States, on the other hand, contains "a patchwork of state and federal constitutional, statutory and regulatory provisions most of which apply to a limited range of commercial activities. In many instances, either because of the absence of legal rights, or because of the nature of the legal provisions themselves, the U.S. system looks to the individual to take action to protect his or her personal information." Id; see also NOLAN, supra note 13, at 3–4 ("[T]he fundamental difficulty in the negotiations as being the ‘major differences in the philosophy of personal data between the US and Europe’. [sic] Europe adheres to much stricter supervision and control on the use of personal data. This elemental difference in philosophy was evident in the attitude of the US negotiators."). Contra Michael Chertoff, Transatlantic Convergence Passenger Data Questions, EUR. AFF. (2008), http://www.europeaninstitute.org/Winter/Spring-2008/transatlantic-convergence-passenger-data-questions.html ("Differences in approach to PNR transfers do exist, largely rooted in culture, geography and history. But their importance and weight have been exaggerated and are now declining in practice. What I've witnessed is a growing convergence among nations—especially among our transatlantic partners—in the battle against terrorism.").

recently noted concerning PNR transfers that, because the United States and the European Union look at privacy differently, the United States is in persistent, intense negotiation battles with the European Union over this issue.\textsuperscript{16} Many in the European legal community argue that, compared to international standards, the United States takes a laissez faire approach to privacy law.\textsuperscript{17} Specifically, critics of the American system argue that it is “sectoral” in its approach, concentrating on a handful of data areas such as medical records or electronic surveillance.\textsuperscript{18} However, “most areas of personal data [are] process[ed] largely unregulated.”\textsuperscript{19}
European nations, on the other hand, claim to "have a 'vision' regarding privacy rights" and take privacy considerations very seriously; some countries have even amended their constitutions to expressly guarantee privacy. The visceral stress given to privacy "may be attributable in part to Third Reich abuses in tracking its target groups with invasive data-collection methods." An instructor at the Washington State Police Academy, from where the author of this Article graduated in 1999, echoed this theory concerning the Nazi regime. The instructor was part of an exchange program with Germany, and one of the major differences he noted between European and American law-enforcement approaches pertained to data collection, specifically that conducted by police in the United States. In Germany, an officer could stop a vehicle for almost any reason and beat the occupant for the slightest of transgressions, but the officer could not write down the offender's name unless he was formally arrested. The instructor explained that, in the United States, an officer must have a "reasonably articulable suspicion" to pull a car over and he cannot rough up a rude passenger. However, the instructor found it amazing that an officer could ask anybody for his or her name and other personal information, write it down, and store that information in a database. The instructor believed that this fundamental difference in attitude between Europeans and Americans was rooted in the use of death lists and domestic spying both in Nazi Germany and in Soviet-ruled Eastern Europe.

As a result of Europe's past, the European Union has enacted broad, prophylactic "omnibus data protection laws covering the full spectrum of uses of personally identifiable information." This resolute attitude toward data security has made data-security laws more comprehensive, reaching "seemingly innocuous databases such as telephone books, restaurant reservations systems, and personal weblogs." In contrast, the United States' sectoral approach is more reactive in nature. Moreover, the United States allows the market to decide how much privacy is

20. Salbu, supra note 12, at 666.
21. Id. at 666–67.
22. Id. at 666; see also Virginia Keyder, Someone in Brussels Should Listen to Ireland, EUOBSERVER.COM (Nov. 26, 2008), http://euobserver.com/22/27181 ("Personal data protection law first arose in Germany, based on a belief that the facility with which pre-war abuses of human rights were carried out was at least partly attributable to the excessive accumulation of personal data by the Nazi regime . . . ").
23. Note that the instructor said this with a sense of drama to make the story more interesting.
24. Givens, supra note 18, at 348–49.
needed, and the public generally has limited statutory rights.26 This self-regulation approach27 is of great concern to privacy-rights advocates because it does not provide an opportunity for the consumer to consent to the data practices of businesses before his information is disseminated.28

Although Nazi terror may be at the heart of why European states have a high concern about privacy rights,29 for the United States, the underlying origin of the “jurisprudential gulf separating the American ‘sectoral’ approach to privacy regulation from other countries’ comprehensive sweep” has roots in the country’s founding document.30 Indeed, because the First Amendment guarantees the right to talk about others by word of mouth, through print, or online, without an exception for speech that violates an individual’s right to privacy, the First Amendment trumps privacy concerns.31 As such, the “Constitution actually protects would-be privacy violators more explicitly than potential victims of privacy breaches.”32 Moreover, it is interesting to note that nowhere in the Constitution or the Declaration of Independence is the word “privacy” or an equivalent word used.33

Conversely, in Europe, “[r]ather than put privacy interests on a scale counterbalanced by free speech rights, these countries analogize privacy rights with intellectual property rights.”34 Stemming from this logic, if the “government is going to let corporations keep competitors from exploiting brand-names and trademarks, the law certainly should allow a citizen to keep others from trafficking in his credit history, sex life and other personal information.”35 The realization of this philosophy in Europe was set forth in the European Union Data Privacy Directive, passed in 1995.36 This directive


29. See Keyder, supra note 22 (“Personal data protection law first arose in Germany, based on a belief that the facility with which pre-war abuses of human rights were carried out was at least partly attributable to the excessive accumulation of personal data by the Nazi regime . . . .”).

30. Forsheit et al., supra note 17, at 17.

31. Id.

32. Id.

33. See generally U.S. CONST.; THE DECLARATION OF INDEPENDENCE (U.S. 1776).

34. Forsheit et al., supra note 17, at 18.

35. Id.

requires each EU member state to enact a data-protection law that covers government, private, and business entities.\textsuperscript{37}

This brings up the central question in this debate: did the conflicting attitudes toward data privacy allow a terrorist like Umar Farouk Abdul Mutallab to board Northwest Airlines Flight 253? In order to answer that question, the history of the debate must be flushed out to understand the backdrop of the problem.

II. HISTORY OF THE LEGAL CONFLICT

To fully understand the dynamics of the United States’ and the European Union’s struggle over PNRs, it is necessary to understand the past of the two sovereigns. Thus, this section will examine the history of the legal battle concerning data privacy.

A. September 11, 2001: Everything Changes

Beyond the death and destruction that the United States witnessed on September 11, 2001, Americans were awakened to the idea that their right to privacy and their freedom to move throughout the country had helped the enemy knock down the World Trade Center and scar the Pentagon.\textsuperscript{38} In addition to deploying the military to fight those responsible for 9/11, the United States recognized that “one of the chief battles of the war on terrorism has been with ourselves, determining to what extent rights and freedoms will be curbed in an effort to save lives.”\textsuperscript{39} The United States was not the only country to be shaken awake by 9/11; at the Extraordinary European Council

\textsuperscript{37} Id.


At the end of the twentieth century, there was relatively little public concern in the U.S. about government use of personal information and much more apprehension about commercial use of data. Accordingly, privacy protection was considered to be more a matter of consumer protection rather than of human rights.

The terrorist attacks in the U.S. on September 11, 2001, changed this. Security suddenly became an overriding concern. Some people in government believed that information technology in general, and data mining practices in particular, could help detect terrorist activity and improve the general safety of the public, the security of the border and the safety of air travel.

Manny, supra note 14; see also Keyder, supra note 22 (discussing the impact of 9/11 on data-privacy protection in the European Union).

\textsuperscript{39} Wyden, supra note 38, at 331.
Meeting on September 21, 2001, the European Union’s Heads of States prioritized the war on terror as a main objective of the European Union and “pledged its support to the US ‘in bringing to justice and punishing the perpetrators, sponsors and accomplices’ of terrorism and issued an action plan against terrorism that contained a broad blue-print of EU counterterrorism activities.”

The either-or paradigm that many proffer concerning privacy and security has proven unrealistic and ultimately protects neither privacy nor security. To that end, 9/11 brought a new reality, which cannot “be met simply with heightened vigilance on both ‘sides’ of a stark equation. Those who bear the responsibility to put security first must understand that if civil liberties are not prominent among their concerns, their efforts may diminish the uniquely American freedoms they seek to protect.” At the same time, defenders of privacy must understand that a proliferation of successful terrorist attacks would weaken the very foundation of the American experience—to prosper and pursue happiness.

Therefore, in order to guarantee the security and the freedom of all Americans, and Europeans for that matter, leaders must embrace an essential principle: “the security of the nation and the protection of individual freedoms are not, and must not be drawn as, mutually exclusive.”

Because commercial airlines were the weapons Al Qaeda used on September 11, 2001, the United States took an immediate interest determining who was entering the nation via passenger airplanes. Hence, in response to the terrorist attacks and this new interest, Congress passed and President H. W. Bush signed the Aviation and Transportation Security Act (ATSA), a law

---

40. NOLAN, supra note 13.
41. See Wyden, supra note 38.
42. Id. “It is difficult to speak about privacy in the United States today without considering the significance of September 11. That day has had a profound impact on the public perception of privacy . . . .” Marc Rotenberg, Privacy and Secrecy After September 11, 86 MINN. L. REV. 1115, 1115 (2002).
43. Wyden, supra note 38, at 331.
44. Id.
Balancing security, privacy, and civil liberties in federal policy is not a finite task; it is a perpetual struggle with a many-headed Hydra. Difficult questions will seldom be permanently settled, and new, uncharted ambiguities will continually arise as America’s anti-terrorism efforts evolve. Since no one solution will end the debate, the best approach for policymakers is to apply intellectual rigor to each new dilemma. Thoughtful leaders will be guided by two bedrock principles: that concerns for security and privacy must be approached in tandem, with neither relegated to an afterthought; and that if a proposed solution abandons one goal for the other, a different solution must be sought.

Id. at 352.
45. Rasmussen, supra note 2, at 567.
that was specifically written to target and prevent future terrorist attacks similar to those by Umar Farouk Abdul Mutallab.47

B. November 11, 2001: The Aviation and Transportation Security Act

One of the first actions that Congress took through the ATSA in response to 9/11 was to federalize airport security.48 As part of this security takeover, Congress required all airlines to provide manifests of passenger data—PNRs—to the U.S. Customs Service in order to compile profiles to combat terrorism.49 The consequences for failing to provide the required information were fines or the revocation of the ability of those airlines to land at airports in the United States.50

Specifically, the ATSA required airlines to gather passenger data on all commercial flights that would fly in U.S. airspace.51 The required PNR had to include the “name, age, country of origin, height and weight, [and] race” of the passengers.52 In addition, the PNR also was required to contain the location of where the passenger was going to stay in the United States, his or her visa information, and any data from the passenger’s purchase of the flight “such as email addresses, credit card numbers, telephone numbers, [and even] dietary

beneficial as not only as a general intelligence gathering mechanism, but also as a measure to increase aviation security. NOLAN, supra note 13, at 4.

49. 49 U.S.C. § 44909(c) (2006). The Department of Homeland Security is also permitted to regulate aircrafts coming to or leaving the United States and demand certain travel documents from passengers under 19 U.S.C. § 1433(c)–(e) (2006). Indeed, all aircrafts must provide advance notification, report their arrival, and meet necessary landing requirements. Id. § 1433(c). In addition, the Customs Service may require an aircraft to provide certain “information, data, documents, papers, or manifests,” as deemed necessary. Id. § 1433(d). Moreover, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 required that the Department of Homeland Security implement a plan to screen passengers and crews of aircraft entering or departing the country. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19 (2004). However, even before IRTPA, airlines had to send an en route electronic transmission with passenger and crew manifests. CBP Proposes Predeparture Passenger and Crew Manifests, 83 INTERPRETER RELEASES 1568, 1568 (2006).
51. 49 U.S.C. § 44909(c). In addition to gathering passenger information, the 9/11 Commission recommended the expansion of “no-fly” lists and the increase of information sharing among federal agencies. 9/11 Report, supra note 38, at 393, 417–18; see also Peter P. Swire, Privacy and Information Sharing in the War on Terrorism, 51 VILL. L. REV. 951, 951 (2006) (discussing how the 9/11 Commission advocated information sharing for security purposes).
preferences.” The information, once transmitted to the authorities, was entered into a computer system that screened the data for potential terrorists.

Because most airlines did not have their own databases for passenger information, most passenger information was stored in a Computerized Reservation System (CRS). The CRS held this data indefinitely, even if the passenger canceled his or her flight.

C. May 28, 2004: Agreement to Transfer

In the past several years, the European Union has developed stringent privacy laws. One such law, Directive 95/46, set out to create European-wide data-protection laws, which included minimum standards with respect to privacy-protection guarantees for each member state. With the exception of France, all EU member states have adopted Directive 95/46. The consequences for noncompliance with the Directive are high and range from severe fines to criminal penalties. For example, in Spain, authorities can levy a fine of between €600 and €60,100 for a minor data-infraction, between €60,100 and €300,500 for moderate infractions, and between €300,550 and €600,000 for serious breaches. In Germany and Denmark, among

53. Id. The PNR also includes residential and business addresses; emergency contacts; hotel reservations; car rental, cruise, and other travel service information; disabilities; and medical conditions. ELEC. INFO. PRIVACY CTRL., PRIVACY & HUMAN RIGHTS 2005: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 80–81 (2005) [hereinafter PRIVACY & HUMAN RIGHTS]. There also exists PNR data on individuals who have never flown before. Edward Hasbrouck, What’s in a Passenger Name Record (PNR)?, THE PRACTICAL NOMAD, http://hasbrouck.org/articles/PNR.html (last visited Oct. 12, 2010).


55. PRIVACY & HUMAN RIGHTS, supra note 53, at 81.

56. Hasbrouck, supra note 53.


59. ROGER BLANPAIN ET AL., THE GLOBAL WORKPLACE: INTERNATIONAL AND COMPARATIVE EMPLOYMENT LAW - CASES AND MATERIALS 325 (2007) ("France was one of the last to adopt revisions to bring its existing Data Protection Act into compliance with the Directive . . . . However, this recently adopted bill has yet to be approved by the French Constitutional Council and may face further modifications. . . . ").


61. Ley Orgánica de Protección de Datos de Carácter Personal [Organic Law on the Protection of Personal Data] art. 45 (B.O.E. 1999, 298) (Spain), available at http://www.boe.es/boe/dias/1999/12/14/index.php (follow “PDF” hyperlink). This is a significant amount of money; as of October 2010, €600,000 translates to $837,382.56. XE: The World’s
other EU states, a violator could face criminal penalties for privacy violations.\textsuperscript{62}

The ATSA put European-based airlines in direct legal conflict with their own Directive 95/46, sparking a transatlantic legal-dispute.\textsuperscript{63} The airlines that complied with ATSA by transferring passenger data violated EU privacy laws;\textsuperscript{64} however, refusal to transmit the data to U.S. authorities meant facing fines and the possible revocation of landing rights.\textsuperscript{65}

The United States and the European Union engaged in talks to resolve the conflict for over a year\textsuperscript{66} and met in Brussels in February of 2003 to finally parley an agreement.\textsuperscript{67} Although the talks between the United States and the European Union failed to reach a comprehensive agreement that resolved the dispute,\textsuperscript{68} the two parties were able to release a joint statement that detailed their progress and announced that an agreement was on the horizon.\textsuperscript{69}


\textsuperscript{63} See HEISENBERG, supra note 52, at 139-40. An illustration of this dispute follows: Following a trip to the US on 26 March 2003, a legal challenge to the interim agreement which resulted from the February talks was taken by a Spanish citizen who was unhappy with the fact that Iberia transferred his PNR data without legal standing. In May 2003, civil rights defenders, European Digital Rights (EDRI) launched a campaign to [sic] against the illegal transfer of European travellers' [sic] data to the US. NOLAN, supra note 13, at 6-7 (footnote omitted).

\textsuperscript{64} Id. at 140.

\textsuperscript{65} Id. at 140-41. Notably, this conflict confused many in the security sector because personal data that concerned public security and defense were considered exempt from the European Directive. Id. at 142. However, because PNRs were compiled for the commercial purpose of flying and only subsequently became relevant for national-security purposes, the exemption did not apply. See id. Thus, "[h]ypothetically, if the data had been collected only for security purposes, they likely would have fallen under the security exemptions . . . ." Id.

\textsuperscript{66} Id. at 142.


\textsuperscript{68} See HEISENBERG, supra note 52, at 142-43.

\textsuperscript{69} Joint Statement, supra note 67.
December 16, 2003, the European Commission on Data Protection and Privacy Matters issued a report to the EU Council and Parliament that outlined its approach to transfer PNRs to the United States.\textsuperscript{70} The Commission’s report proffered a system wherein the United States would agree to: 1) only require thirty-four pieces of information with every PNR; 2) destroy sensitive data; 3) only use the PNR to prevent terrorism or other related crimes; 4) only retain the PNR for three and one-half years; 5) allow involvement of EU privacy authorities; and 6) participate in an annual review of the agreement.\textsuperscript{71}

On May 14, 2004, the European Commission found that the United States had given proper assurances that it would protect PNR data.\textsuperscript{72} As a result, on May 17, 2004, the EU Council approved the conclusion of the Commission.\textsuperscript{73} Subsequently, on May 28, 2004, the United States and the European Union signed an agreement concerning the transfer of PNRs that followed the Commission’s September 16, 2003 report.\textsuperscript{74}

\textbf{D. May 30, 2006: The European Court of Justice Rejects the Agreement}

On July 27, 2004, the European Parliament appealed to the ECJ asking the court to annul the EU Council’s decision that found that the United States had given the proper assurances.\textsuperscript{75} Specifically, the Parliament argued that

\begin{itemize}
  \item \textsuperscript{71} Id. The report also distinguished between a system of data transfers in which the airlines would transmit data to the United States, and a system in which the European Union would control and filter the data the United States could access. Id. The Commission strongly advocated for the latter system. Id.
  \item \textsuperscript{72} Commission Decision 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 2004/535/EC, art. 1, 2004 O.J. (L 235) 11, 13.
  \item \textsuperscript{73} Council Decision 2004/496/EC, art. 1, 2004 O.J. (L 183) 83, 83.
  \item \textsuperscript{75} Press Release, European Court of Justice, The Court Annuls the Council Decision Concerning the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of Personal Data and the Commission Decision on the Adequate Protection of Those Data (May 30, 2006) [hereinafter European Court of Justice], available at http://curia.europa.eu/en actu/communiques/cp06/aff/cp060464en.pdf. The European Parliament, which is elected by citizens, shares power with the European Council. The European Parliament, EUROPA, http://europa.eu/institutions/inst/parliament/index_en.htm (last visited Oct. 12, 2010). The Parliament shares its power over the budget with the Council, but the Parliament can “adopt or reject the budget in its entirety.” Id. Although the Council is considered on equal footing with the Parliament, “[i]n some fields (for example agriculture, economic policy, visas and immigration), the Council alone legislates, but it has to consult
adoption of the decision on adequacy was ultra vires, because the EU Council did not have the authority to make the agreement and fundamental rights had been infringed. The ECJ, on May 30, 2006, accepted the Parliament’s petition and annulled both the Council’s decision and the Commission’s report that found the United States’ assurances adequate. The ECJ gave the interested parties until September 30, 2006, to establish a new agreement.

In ruling against the Commission’s report, the ECJ reasoned that, under European law, the PNR data did not fall within the exception for data collection for security or defense purposes. This was chiefly because PNR data was not collected by the airlines for security or defense reasons, but rather for commercial purposes; thus, the security-defense exception reasoning cited in the Commission’s report did not apply.

In permitting the transfer of the PNR to the United States, the European Council cited to authority under article 25 of the Data Directive that allowed for the transfer of data to third countries if the country could provide adequate assurances that the data would be protected. However, like the decision against the Commission, the ECJ found that, because the underlying bases of the Council’s decision were outside the scope of the Data Protection Directive, the agreement had no appropriate legal basis and was, accordingly, annulled.

E. July 23, 2007: A New Agreement Is Reached

Because of the ECJ’s May 30, 2006 decision, the United States and the European Union rushed to reach an interim agreement and did so in October
The interim agreement had an expiration date of July 31, 2007, giving the United States and the European Union less than one year to reach a formal agreement that complied with the ECJ ruling. On July 26, 2007, a mere five days before the interim agreement expired, a Revised Agreement was finalized.

Accompanying the Revised Agreement was a “letter by [the U.S. Department of Homeland Security] giving assurances on the way it intended to protect PNR data . . . .” Additionally, the Revised Agreement required a “reply letter from the [European Union] . . . confirming that on the basis of the assurances, it consider[ed] the level of protection of PNR data in the United States as adequate.”

In order to comply with the ECJ decision, the European Union changed the legal basis for the agreements—first in the Interim Agreement and then in the final Revised Agreement. The original basis for the first agreement was the Treaty Establishing the European Community, or the “first pillar,” which the ECJ rejected. The new legal reasoning was based on the Treaty on European


87. Id. at 837–38 (internal quotation marks omitted). The new agreement is set to expire in seven years unless both parties agree to extend or replace it, or one party decides to terminate the agreement. Revised Agreement, supra note 85, at 19.

88. VanWasshnova, supra note 1, at 838; see Revised Agreement, supra note 85, at 18; Interim Agreement, supra note 83, at 29.

89. VanWasshnova, supra note 1, at 838.
Union, or the "third pillar."\textsuperscript{90} "As a result [of the change], the Revised Agreement now falls under the competence of the European Union, as opposed to the European Community."\textsuperscript{91}

Although the Revised Agreement did not provide all the safeguards the European Parliament insisted upon, it did incorporate several significant insurance provisions that were absent from the original agreement.\textsuperscript{92} "For instance, the Revised Agreement extend[ed] the privacy protections found in the Privacy Act of 1974 and the Freedom of Information Act to non-U.S. citizens and provide[d] a system of redress for persons seeking information about . . . PNR[s]."\textsuperscript{93} The Revised Agreement also provided assurances from the United States that the Department of Homeland Security (DHS) would "provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display [and] . . . w[ould] work with interested parties in the aviation industry to promote greater visibility of this notice. Finally, the Revised Agreement adopt[ed] the ‘push’ system of transmitting PNR," discussed in detail below.\textsuperscript{94}

III. BALANCING COUNTERVAILING POSITIONS

Not long after the Revised Agreement was signed, critics started opining on its legality and possible legal challenges.\textsuperscript{95} Interestingly, before the ink was dry on the Revised Agreement, the European Union started drafting its own internal PNR-sharing law; this, too, has raised serious legal questions.\textsuperscript{96} Beyond these challenges are the two threshold questions at issue here: 1) Do PNR transfers increase national security and, if they do, is the legal wrangling concerning PNR transfers jeopardizing that security; and 2) Has a proper balance been struck between privacy and national security concerns with regards to PNR transfers?

\textsuperscript{90} Id.; see Revised Agreement, supra note 85, at 18–19; Interim Agreement, supra note 83, at 29–30; see also Consolidated Version of the Treaty on European Union, arts. 1–2, Dec. 24, 2002, 2002 O.J. (C 325) 5.

\textsuperscript{91} VanWasshnova, supra note 1, at 838.

\textsuperscript{92} Id.

\textsuperscript{93} Id.

\textsuperscript{94} Id.

\textsuperscript{95} See, e.g., VanWasshnova, supra note 1, at 838; Letter from Peter Hustinx, Eur. Data. Prot. Supervisor, to Dr. Wolfgang Schäuble, Minister for the Interior, Ger. (June 27, 2007) (on file with author).

A. New Challenges

Although the July 23, 2007 agreement increased some privacy protections over PNRs, many critics argue that the Revised Agreement abated protections in other areas. First, the Revised Agreement nearly quintuples the time the United States can retain PNR information from three and one-half years to fifteen years. Second, DHS may now use PNR information pertaining to race, ethnicity, political affiliation, religion, union membership, health, and even an individual's sex life. Finally, critics of the new agreement argue that, although the Revised Agreement reduced the number of data inquiries from thirty-four to nineteen, the "change is a mere subterfuge as the Revised Agreement groups all but one of the thirty-four elements into one of nineteen new data sets." Also, the Revised Agreement appears to solve the push-pull debate, in which the "pull" method allows U.S. authorities access to airline reservation systems, and the "push" method permits airlines to send requested information to U.S. authorities. Yet, critics of the agreement contend that this fix is a gambit. Additionally, there is concern that the United States will suspend the ability of European air carriers to operate in U.S. air space, thus pressuring airlines to abide by other requests, even those that are outside the scope of the Revised Agreement.

98. Id. The agreement also contains a provision to extend the retention time past the fifteen-year mark. Id.
Under the Revised Agreement, data is stored in an active analytical database for seven years and then moved to dormant, non-operational status for eight years, where it can be "accessed only with approval of a senior [Department of Homeland Security] official . . . and only in response to an identifiable case, threat, or risk. After the fifteen year period has expired, the Department of Homeland Security expects that the data will be deleted, and the Revised Agreement states that "questions of whether and when to destroy PNR data . . . will be addressed . . . as part of future discussions."
Id. at 839 n.82 (citation omitted).
99. Id. at 839.
100. Id. Critics also argue that "the Revised Agreement requires the airlines to transfer new PNR data that were not required under the previous agreements, including additional baggage and frequent flyer information." Id.
101. Id. at 838; see also Proposal for a Council Framework Decision of 6 November 2007 on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, EUROPA, [hereinafter EU PNR Proposal], http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/114584_en.htm (last updated May 2008). The push method is "the method under which air carriers transmit the required PNR data into the database of the authority requesting them," and the pull method is a "method under which the authority requiring the data can access the air carrier's reservation system and extract a copy of the required data into their database." Id.
102. See VanWasshnova, supra note 1, at 838–39 (arguing that despite the safeguards incorporated into the Revised Agreement, the agreement still does not "adequately provide privacy protections").
103. Id. at 858–59.
Although formal legal action has not been initiated against the Revised Agreement, such an action may be on the horizon. In an official report to Congress, the Library of Congress’s Congressional Research Service opined that “European Parliamentarians and European civil liberty and privacy groups may still challenge the new July 2007 PNR agreement.” Moreover, the report points out that the PNR debate has heightened general European concern with data security.

In a press release, the European Parliament stated that the Revised Agreement is substantially flawed and fails to protect citizens’ personal data. Similarly, Peter Hustinx, the European Data Protection Supervisor, has “grave concern[s]” that he detailed in a letter to Dr. Wolfgang Schäuble, Germany’s Minister for the Interior. Specifically, Mr. Hustinx is distressed over the following issues:

- The extension of the time that passenger data are kept—effectively from 3.5 [sic] to 15 years in all cases—introducing a concept of “dormant” data that is without legal precedent;
- Data on EU citizens will be readily accessible to a broad range of US agencies and there is no limitation to what US authorities are allowed to do with the data;
- The absence of a robust legal mechanism that enables EU citizens to challenge misuse of their personal information; and
- The US wants to avoid a binding agreement by exchange of letters.

In what appears as a precursor to formal litigation, the Members of the Alliance of Liberals and Democrats for Europe made an article 255 request, the European equivalent of a Freedom of Information Act request, for “all the documents related to . . . the negotiation of the 2007 Agreement between the European Union and the United States of America on the processing and transfer of passenger name record[s] . . . as well as [access] to the documents related to the confidentiality of negotiations documents.”

---

105. Id.
107. Letter from Peter Hustinx to Dr. Wolfgang Schäuble, supra note 95.
108. Id.
European organizations were not the only ones unsettled by the Revised Agreement. Indeed, in a letter to Michael Chertoff, the former Secretary of the U.S. DHS, the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) expressed “concerns about the possible collection and retention of information indicating the union affiliation of air passengers and the use of that information to determine whether a person poses a terrorism security risk.” The AFL-CIO went on to reject the idea that union affiliation has any bearing on whether an individual is a security threat. Consequently, the AFL-CIO requested that the Department “state clearly that it will not collect information on union membership and will ensure that this information is deleted from PNR data before it is transferred to DHS.”

Despite the criticism, there was an immediate response from the leadership within the European Union and from the DHS supporting the PNR agreement after the failed terrorist attack on December 25, 2009. Specifically, the two sovereigns released U.S.-EU Joint Declaration on Aviation Security on January 21, 2010. The Declaration stated that the European Union, the European Commission, and the Secretary of the DHS, Janet Napolitano, met in Toledo, Spain, and “discussed current terrorists threats, in particular the attempted attack on an aircraft approaching Detroit on 25th December 2009, ways to strengthen international security measures and standards for aviation security, and an upcoming global dialogue on securing international travel.” The group declared that the “last attempted attack on 25th December by an individual who flew from Africa to the United States via Europe highlights the international nature of this threat. An international threat demands an international response.” Among other countermeasures, the meeting participants agreed to “[c]ontinue the excellent cooperation between the EU and the United States on aviation security issues based on the EU-U.S. Air Transport Agreement.” In addition, the parties agreed that the European Union and the United States should draw on the lessons learned from the Revised Agreement and continue to review how the “use of passenger information in the prevention of terrorism in considering what and how operational cooperation sharing could be further improved and compatible

111. Id.
112. Id.
113. Id.
115. Id.
116. Id.
117. Id.
118. Id.
approaches could be developed among partners committed to aviation security, the rule of law, and international human rights.”

In the EU-U.S. Joint Statement on Enhancing Transatlantic Cooperation in the Area of Justice, Freedom and Security, the commitment to the PNR agreement was also reinforced. In this declaration, the PNR agreement was touted as a success, and the European Union and United States committed to “undertake joint reviews of the agreement in order to assure the effective operation and privacy and personal data protection of [their] respective systems for collecting and analyzing such data.” However, though the official statements seem to indicate that the PNR agreement is not in jeopardy, the European Union and individual nations within the Union have taken steps that directly call into question the future of this important agreement.

Germany recently took such a step when its constitutional court overturned a 2008 law. The law, designed to combat terrorism and serious crimes required communications data to be stored for six months. In its decision to overturn the law, the court ordered the deletion of the vast amounts of stored data, stating that the “law [w]as a ‘particularly serious infringement of privacy.’”

Even more troubling to supporters of the PNR agreement is the EU Parliament’s recent rejection of the Terrorist Finance Tracking Program (TFTP). Many in the national-security arena believe this is not only a major blow to U.S.-EU relations, but that it also makes both sovereigns less safe.

In fact, in a plea to the EU Parliament before it voted to reject the agreement, the U.S. Treasury Under Secretary for Terrorism and Financial Intelligence, Stuart Levy, wrote to the Parliament arguing that rejecting the law would make citizens in both the United States and the European Union less safe.

Mr. Levy stated,
The TFTP has been instrumental in protecting the citizens of the United States and Europe, and it has played a key role in multiple terrorism investigations on both sides of the Atlantic. To take but one example, TFTP information provided substantial assistance to European governments during investigations into the Al Qaeda-directed plot to attack transatlantic airline flights traveling between the EU and the United States. TFTP information provided new leads, corroborated identities, and revealed relationships among individuals responsible for this terrorist plot. In September 2009, three individuals were convicted in the UK, and each was sentenced to at least thirty years in prison.¹²⁹

Mr. Levy concluded his op-ed by arguing that rejecting the TFTP would handicap the ability of both the United States and the European Union to track and prevent terrorism, and that losing the TFTP would be a “regrettable and potentially tragic mistake.”¹³⁰

Despite the precarious status of the U.S.-EU agreement, a possible EU PNR law is on the horizon, though it likely faces challenges.

B. New Laws?

On November 6, 2008, the European Commission tendered a proposal to establish a PNR system and collect personal data on everyone flying into and out of EU member states.¹³¹ The new law, if enacted, will require data that “is almost exactly the same as that being collected under the controversial EU-US PNR scheme.”¹³² The data that is collected will be retained as “active” for five

¹²⁹. Id. Mr. Levy also commented that “[u]ndetected and undeterred, terrorists will abuse the integrity and openness of the world’s financial system. The benefits of the Terrorist Finance Tracking Program have been incalculable in enhancing the safety and well-being of European and American citizens.” Id.

¹³⁰. Id.

¹³¹. PNR Scheme, supra note 11.

¹³². Id. The data collected under the new law includes:

(1) PNR record locator; (2) Date of reservation/issue of ticket; (3) Date(s) of intended travel; (4) Name(s) [sic]; (5) Address and Contact information (telephone number, e-mail address); (6) All forms of payment information, including billing address; (7) All travel itinerary for specific PNR; (8) Frequent flyer information; (9) Travel agency /Travel agent [sic]; (10) Travel status of passenger including confirmations, check-in status, no show or go show information; (11) Split/Divided PNR information; (12) General remarks (excluding sensitive information); (13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields; (14) Seat number and other seat information; (15) Code share information; (16) All baggage information; (17) Number and other names of travellers [sic] on PNR; (18) Any collected API information; and (19) All historical changes to the PNR listed in numbers 1 to 18.
years, whereas the Revised Agreement with the United States provides that data will be retained for seven years. Both the Revised Agreement and the proposed law, however, provide that data may be kept for eight additional "dormant" years after the active period. Thus, the United States could hold data for a total of fifteen years under the Revised Agreement and thirteen under the proposed EU law. And, as noted, the actual information collected is virtually identical to the information collected under the Revised Agreement.

The European Union's Interior Ministers have already given their support of the proposed law. The official motivation, according to the Commission's impact assessment, for the EU PNR law was twofold:

[1] An EU-wide PNR system would improve security by, in particular, preventing changing of travel patterns of passengers to Member States with no PNR and enhancing information exchange between Member States.

[2] Increase legal certainty and reduce costs for air carriers by fostering common standards for transmission of PNR data and by preventing distortions of competition arising from possible differences in various national PNR requirements incumbent on carriers.

According to the European Union Home Affairs Commissioner, Jacques Barrot, the plan was to have the law passed and running by the end of 2009. Despite the support from the Commission and the Interior Ministers, the new
scheme has come under attack from the European Parliament. Specifically, the European Parliament issued a press release on November 20, 2008, stating that it “stands against a plan to collect air passenger records for law enforcement purposes that could pose a threat to privacy.” Moreover, the Parliament adopted a resolution by an overwhelming majority that criticized the Commission’s proposal. Additionally, the members of the Parliament found that “the measure was not justified legally, as well as in terms of effectiveness in the fight against terrorism. They ask[ed] for evidence that such a system would be useful at EU level, and could not vote on the text until their many concerns ha[d] been addressed.”

These comments from the European Parliament have been given a whole new meaning with the passage and implantation of the Lisbon Treaty. Before the EU PNR law could go into effect, it was put on hold because the potential enactment of the new Lisbon Treaty. The European Union’s member states quickly signed the Treaty on December 13, 2007, and it went into force on December 1, 2009. The Treaty created significant changes, including granting more power for the European Parliament in legislative issues, giving them “equal footing” with the Council of Ministers; redistributing “voting weights between the member states”; and prohibiting the use of national vetoes for certain topics.

This new “role” for the European Parliament is significant with regards to PNR transfers because Members of the Parliament have been very critical of both the United States’ and the European Union’s PNR transfer agreements.

---


141. Id.

142. Id. (noting that the resolution was adopted with “512 votes in [favor], 5 against and 19 abstentions”).

143. Id.

144. Press Release, Passenger Name Record Talks on Hold, supra note 12.


147. Press Release, Passenger Name Record Talks on Hold, supra note 12 (“On several occasions, MEPs voiced serious criticism of the proposed EU PNR scheme, a plan to collect air passenger records for law enforcement purposes, ‘essentially copying a scheme applied in the US’. . . .”).
To date, because of the Lisbon Treaty, there has not been any real movement on the European PNR law.  

U.S. national-security officials are concerned that, because the PNR agreement was not fully ratified before the Lisbon Treaty took effect, that agreement, as with the TFTP agreement, may be in trouble. Indeed, commentators on U.S./EU privacy relations believe that the PNR agreement may be next in Parliament's cross-hairs. One such commentator recently stated that the "European Parliament is already beginning to consider whether to ratify another . . . 'agreement' . . . [on] Passenger Name Records (PNRs) containing airline reservations and other travel data." That, as with the TFTP, the Lisbon Treaty has given Parliament new power that it is willing to use, and that the TFTP and PNR agreement share similar histories—specifically that Parliament has resisted them since their conception—indicates that the PNR agreements may be threatened. In addition, U.S. government officials are worried that the agreement may come under attack from Parliament. Ivan Fong, General Counsel for the DHS, was recently asked at a national-security conference whether the PNR scheme was in jeopardy because of the Lisbon Treaty and the Parliament's past criticism of the PNR-sharing agreement. Mr. Fong answered that, although Europeans and the United States view privacy differently, "I'm an optimist, I think we can bridge some of those differences. I think we share many of the same end goals." However, Mr. Fong went on to say that "recent events suggest that there is some risk that the PNR sharing agreements that we have will have to be revisited in the light of the current and recent actions."

C. Balancing Security of Data with Security of a Nation

The fundamental objective of the European Union, since the adoption of the Treaty of Amsterdam, "has been to provide citizens with a high level of security within an area of freedom . . . and justice." Since the terrorist attacks of September 11th, the attacks in Madrid and London, and the most recent attempted Christmas-Day attack on Flight 253 (originating in Europe),

149. See id.
150. See id.
151. See id.
152. See id.
153. See, e.g., Fong, supra note 9 (acknowledging that the agreement may be in jeopardy of being overturned).
154. Id. The author of this Article asked Mr. Fong this question.
155. Id.
156. Id.
157. NOLAN, supra note 13, at 2 (internal quotation marks omitted).
the European Union has earnestly increased its efforts to provide security and liberty to its citizens.158 Yet, under the guise of the war on terror, many argue that the European Union, under pressure from the United States, has placed a greater emphasis on physical security, while neglecting privacy security.159 Indeed, guarding fundamental freedoms while simultaneously protecting national security and the lives of the citizenry is not easy to balance.160 Critics of the European Union’s current approach contend that looking at “PNR transfer as an example of the EU’s adoption of counter-terrorism polices, does not instill confidence in the EU’s commitment to ensuring that its approach in tackling terrorism is reconciled with respect for the fundamental freedoms which form the basis of our civilisation.”161 These critics also argue that “freedoms of natural persons with regard to the processing of personal data were ignored in the case of PNR data transfer [and] is an issue of grave concern for the EU citizen.”162 These criticisms are similar to those in the United States, where commentators argue that the PNR-transfer agreement does not adequately “protect the privacy of airline passengers, that the United States should adopt stricter privacy laws, and that it is further necessary to establish an international standard for the global protection of airline passenger data.”163

However, in order to successfully fight terrorism, nations must seize the opportunity to identify terrorists and other international criminals during one of the few occasions when they must expose themselves to the international community—when they board an aircraft.164 This was the very case with Mutallab, who was on the international radar because of warnings from his father, but whose whereabouts were unknown until he stepped on Northwest Airlines Flight 253.165

Recognition of this opportunity is the motivation behind the United States, and now the potential new European Union, laws regarding PNR transfers.166 Identifying these individuals through information provided to the airlines unquestionably has challenges. Mr. Chertoff, when speaking as the Secretary of Homeland Security, stated that the United States receives ninety-one million

158. Id.
159. Id.
160. Id. at 11.
161. Id. (internal quotation makes omitted).
162. Id. at 12.
164. VanWasshnova, supra note 1, at 864.
166. See VanWasshnova, supra note 1, at 864.
travelers by air each year.\footnote{167} The good news, Secretary Chertoff pointed out, "is that only a tiny handful might pose a genuine threat; the bad news is that, given modern technology, it only takes a few to wreak untold havoc."\footnote{168}

Thus, while the United States possesses "terrorist watch lists that identify people we know to be dangerous, we need to find individuals who are terrorists but are not yet known to us. The question is how best to do it without taking the kinds of draconian measures that would shut down travel altogether."\footnote{169} The former Secretary identified data mining as a key area to combat these terrorists.\footnote{170} He cited to the European Union’s PNR agreement as an important tool because, "[b]y collecting just a few key pieces of non-sensitive, commercial information, we can identify the small number of passengers who warrant a closer look before they board a plane or enter our country."\footnote{171}

Data-mining has had some success: In April 2006 at Boston’s Logan Airport, two arriving passengers exhibited travel patterns indicating "high-risk behaviors" and so Customs and Border Protection (CBP) officers decided to take a closer look at them. In the "secondary interview" process, one subject stated that he was traveling to America on business for a group suspected of having financial ties to Al Qaeda. When his baggage was examined, officers discovered images of armed men, one of them labeled "Mujahadin." Both passengers were refused entry to the United States.

Three years earlier, on the basis of such data and other analytics, an inspector at Chicago’s O’Hare Airport pulled aside an individual for secondary questioning. When his answers did not satisfy the security officers, he was denied U.S. entry - but not before his finger-prints had been taken. The next time we saw those fingerprints or rather parts of them, they were on the steering wheel of a suicide vehicle that blew up and killed 32 people in Iraq.\footnote{172}

Despite the advantages of data mining, Secretary Chertoff recognized during his tenure at the DHS that critics saw the tactic of data mining passenger information "as evidence that the United States is grabbing every available piece of information, acting like Big Brother and acting alone in this manner on the world stage."\footnote{173} At the same time, however, Secretary Chertoff asserted that the United States, and other democratic countries that have implemented similar programs concerning PNR transfers, understand the value of privacy and balance the need for data security with the need for national security.\footnote{174}

\footnotesize
\textsuperscript{167} Chertoff, supra note 14.
\textsuperscript{168} Id.
\textsuperscript{169} Id.
\textsuperscript{170} See id.
\textsuperscript{171} Id.
\textsuperscript{172} Id.
\textsuperscript{173} Id.
\textsuperscript{174} See id.
The EU Commissioner, Franco Frattini, has echoed Secretary Chertoff’s position. When speaking on the draft EU PNR law, Commissioner Frattini stated that it would be “strange if we didn’t then also concern ourselves with Europeans’ security.” These are important words from Commissioner Frattini who has been an outspoken advocate on the importance of privacy security.

However, not everyone agrees with Secretary Chertoff that PNR transfers increase national security. The Members of the European Parliament (MEP) have stated that “no evidence [exists] of the usefulness of the mass collection and use of PNR data for counter terrorism purposes...” Addressing the new EU PNR law, the MEP argue that, because the law has “a considerable impact on the personal life sphere of European citizens,” the fact that it may or may not increase security is not sufficient. Ultimately, the

---


176. Id.


178. See Press Release, MEPs Voice Serious Criticism, supra note 140.

179. Id. The Parliament does acknowledge that PNR transfers do “provide evidence of its usefulness for other purposes, as well as the value of using PNR on a case-by-case basis in the context of ongoing investigations, and on the basis of a warrant and with due cause.” Id.

180. See id. The MEPs also note that “the European Court of Justice already challenged the EU-US PNR agreement on this ground. They therefore decide[d] to reserve their formal opinion on the framework-decision once their concerns have been addressed.” Id. Additionally, a commission of the European Council charged with “present[ing] a common EU approach on the use of passenger data for law enforcement purposes” offered the following discussion on the necessity of a standard European PNR system:

- Is processing of PNR data useful and needed to effectively increase security in the EU?
- On the basis of the experience gained, for example, in the USA and the UK, we should be able to establish whether the proposal is necessary for the purpose sought, i.e. to effectively increase the level of security in the fight against terrorism and organised [sic] crime, in particular in view of the possible interference with civil liberties.

- Is there a need for an EU PNR system?
- Action on the EU level should be necessary and should present advantages over no EU action scenario, where some Member States would put in place their national PNR systems. The EU added value could be perceived from the security, business and data protection perspective.

As to security, it remains open whether national PNR systems could provide for a sufficient coverage of passenger flows and an efficient exchange of information between Member States’ competent authorities. National approaches may also lead to changes in travel patterns of passengers towards the EU Member States which do not process PNR data.

From the business perspective, a set of diverging national PNR systems could also be perceived inferior to an EU system in terms of administrative costs, legal certainty and level playing field.
MEP question the conditions that make the new PNR law necessary and express concern that “the proposal would give authorities warrantless access to all data while their added value for law-enforcement purposes has not been proved, as there is no evidence that PNR data are useful for massive profiling or data mining in order to seek potential terrorists.”

To balance privacy with national security, MEP argue that the European Union’s PNR law should be used only “on a case-by-case basis, in the context of ongoing investigations.”

But this raises the obvious question of who determines if a certain situation meets whatever “need” threshold has been established? Does a tribunal of some type make this determination? Does the sovereign nation in which the airplane is landing make this determination or does the nation from where the airplane departed? Is not the whole point of automatic PNR data transfers to keep up the national security need of fast intelligence? All of these questions point to the central problem with a case-by-case approach to PNR data sharing—unanswered questions of who and when?

Furthermore, the many member states and other pertinent organizations contend that, in the event that PNR information is used by law enforcement, it should be for the limited scope of preventing terrorism and defeating organized crime. If the field is too broadly defined, they argue, “the interference with the right to privacy is no longer justified by the ends it seeks to achieve. On the other hand, if the field of use is defined too narrowly, its contribution to the public security can be insignificant.” In essence, all parties to this deliberation argue that privacy must be balanced with security; the question to be answered, and the question that will continue to ignite debates, is where the line should be drawn.

In the end, this is a difficult issue with no bright-line rules to give easy answers. However, what is clear is that the less the international community cooperates, the less safe the world will be; the less intelligence that is shared, the less safe the world will be; the more bureaucratic hoops that are made, the

From the data protection perspective, an EU instrument guarantees that the passenger data gathered are subject to harmonised [sic] data protection rules throughout the European Union.


Press Release, MEPs Voice Serious Criticism, supra note 140. MEPs suggest that “better results could be obtained by improving mutual legal assistance between law enforcement authorities.” Id. (internal quotation marks omitted). Furthermore, MEPs advocate that the “new legislation should include a sunset clause and estimate that the need for action at the community level has not been sufficiently demonstrated, nor the proportionality of the measure.” Id.

MEPs also say the proposal should also create a burden for air carriers, and that they should not be required to collect additional data or be made responsible to verify the records.” Id.


MEPs also say the proposal should also create a burden for air carriers, and that they should not be required to collect additional data or be made responsible to verify the records.” Id.

Id.
less safe the world will be; and the more time and resources that are spent on
meeting artificial legal requirements, the less safe the world will be.

IV. CONCLUSION

One of the first things that DHS Secretary Janet Napolitano did after the
attempted terrorist attack on Christmas Day 2009 was to fly to Europe and talk
to EU transportation authorities. The purpose of her trip, among other
issues, was to emphasize how important PNR information is to the United
States and to emphasize to the world that the United States takes security
seriously. However, in a time when the United States and the rest of the
international community are constantly reminded of the threat that terrorism
leaves at the world’s doorstep—the most recent reminder being this past
Christmas Day—and when “exceptionality” has become the norm, the world
must be vigilant to assure that liberty is not compromised in the name of safety
in the effort to wage this important war on terror.

It is not entirely clear if the original U.S.-EU PNR agreement or any changes to the PNR agreement
now or in the future would have impacted December 25, 2009; what is clear,
however, is that this incident reinforced how important the information is.

Striking the proper balance between privacy and a country’s need to protect
national security has been an extremely contentious issue since the attacks on
September 11, 2001. It was not long after 9/11 that Congress passed
legislation that bolstered national security. “Laws such as the Patriot Act
bartered privacy interests for the promise of increased security. With the
passage of time, however, these nationalistic sentiments have decreased. Civil
liberty advocates are now questioning the necessity and effectiveness of
national security measures that infringe upon privacy rights.”

[185] Press Release, U.S. Dep’t of Homeland Sec., U.S.-EU Joint Declaration on Aviation
Security (Jan. 21, 2010), available at http://www.dhs.gov/ynews/releases/pr_1264119013
710.shtm.
[186] Id.
[188] The role of national democratically elected parliaments, the European Parliament and
civil rights commentators has arguably never been more important.
As Den Boer and Monar warned us, we need to be careful that counter-terrorism efforts
within the EU do not ‘contribute to a complete domination of EU justice and home
affairs by an all-encompassing security rationale.[sic](which) if left unchecked, . . .
[sic] could ultimately reduce one of the most ambitious political projects of the EU of
recent years, the ‘area of freedom, security and justice’, [sic] to that of a mere
integrated law enforcement zone’. [sic]

Id.

[189] Irfan Tukdi, Comment, Transatlantic Turbulence: The Passenger Name Record
[190] Id. (footnote omitted).
However, the act of transferring PNR data does not compromise the privacy rights of citizens of the world to the level that completely abandoning the current PNR regime would reduce the security it provides. PNR transfers appropriately focus on identifying suspected terrorists and international criminals when they expose themselves to the international community. It is true that, if the objective is to eliminate all risk, it is a quixotic goal; thus, nations instead must endeavor to manage their risk. This is important because nations that pursue complete risk elimination ultimately seem to harm the very thing they were trying to protect. The United States “could eliminate every risk to our airliners by shutting down our airports, but that would hand the terrorists a victory by destroying air travel—just what the terrorists were trying to achieve in the first place by attacking our airliners.”

As such, both the United States and the European Union must strike a careful balance between tracking down terrorists and international criminals, and the protection of privacy rights. The saying that the ends never justify the means only holds true if one is alive to criticize the means.

191. VanWasshnova, supra note 1, at 865.
193. Id.
194. Id.
195. VanWaschhova, supra note 1, at 865.