

COMMENT

TRANSATLANTIC TURBULENCE: THE PASSENGER NAME RECORD CONFLICT*

TABLE OF CONTENTS

I.	INTRODUCTION	588
II.	APPROACHES TO SECURING DATA PRIVACY IN THE EUROPEAN UNION AND THE UNITED STATES	591
III.	PENALTIES OR PROSECUTION?.....	593
	A. <i>State of Passenger Screening</i>	594
	B. <i>The No-Win Dilemma of the European Airlines</i>	597
IV.	NEGOTIATING A SOLUTION	598
	A. <i>Joint Statement and Parliament's Initial Objections</i> ...598	
	B. <i>CBP Undertakings and EU Adequacy Finding</i>	601
	C. <i>Agreement and Parliament's Challenge</i>	604
	D. <i>The ECJ Annulment</i>	606
	E. <i>Recent Developments</i>	610
V.	TWO PROPOSED STRATEGIES: DEVELOPING A MULTILATERAL FRAMEWORK OR ABANDONMENT OF THE USE OF PNR DATA.....	611
	A. <i>A Multilateral Framework</i>	611
	B. <i>Eliminate the Role of PNR Data in Passenger Screening</i>	614
	1. <i>The Use of PNR Data Is Ineffective</i>	614

* This Comment received the King & Spalding LLP Award for the Best Student Paper in the Area of International Business. The Author would like to acknowledge the assistance of Professor Chenglin Liu in selecting the topic of this Comment, and thank the editors and staff of the *Houston Law Review* for their generous contributions. Additionally, the Author thanks his parents for their unyielding support, his brother for his invaluable counsel, and his wife for her loving dedication and friendship.

2. *Civil Liberties Concerns*.....615
 3. *Adequate Safeguards Exist*.....617

VI. AN IMPERFECT SOLUTION.....619

VII. CONCLUSION.....619

I. INTRODUCTION

In the aftermath of the September 11, 2001 terrorist attacks, Congress passed broad legislation to address the nation’s security concerns.¹ Congress’s swift response to the attacks included legislation aimed at revamping federal aviation security regulations and protecting the tattered airline industry from further harm.² Within two weeks of the attacks, Congress adopted the Air Transportation Safety and System Stabilization Act (ATSSSA); a few months later, Congress enacted the Aviation and Transportation Security Act (ATSA).³ The ATSA authorizes creation of the Transportation Security Administration (TSA) and charges this agency with developing new aviation security guidelines and procedures.⁴ The ATSA further mandates that airlines traveling to or from the United States provide passenger flight manifests and certain passenger name record (PNR) information to the Bureau of Customs and Border Protection (CBP).⁵ PNR information includes, among other items, passengers’ names, credit card information, and even meal preferences.⁶ Airlines failing to comply with the

1. Frederic Block, *Civil Liberties During National Emergencies: The Interactions Between the Three Branches of Government in Coping with Past and Current Threats to the Nation’s Security*, 29 N.Y.U. REV. L. & SOC. CHANGE 459, 471–78 (2005).

2. See generally Richard P. Campbell, *America Acts: Swift Legislative Responses to the September 11 Attacks*, 69 DEF. COUNS. J. 139 (2002) (documenting legislative efforts aimed at protecting the airline industry from economic and legal harm following the September 11 attacks).

3. Air Transportation Safety and System Stabilization Act, Pub. L. No. 107-42, 115 Stat. 230 (2001) (codified as amended at 49 U.S.C. § 40101 note (Supp. IV 2004)); Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified as amended in scattered sections of 5 U.S.C., 26 U.S.C., 31 U.S.C., and 49 U.S.C.); see also Campbell, *supra* note 2, at 140–45 (analyzing the ATSSSA and the ATSA).

4. Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101, 115 Stat. 597, 597–604 (2001) (codified as amended in scattered sections of 5 U.S.C. and 49 U.S.C.) (establishing the TSA and granting it authority over civil aviation security).

5. 49 U.S.C. § 44909(c) (Supp. IV 2004) (requiring airlines to disclose the name, date of birth, citizenship, gender, passport number and country of issuance, and other information of passengers and crew that is “reasonably necessary to ensure aviation safety”).

6. Megan Roos, Note, *Definition of the Problem: The Impossibility of Compliance*

2008] *THE PASSENGER NAME RECORD CONFLICT* 589

ATSA's disclosure requirements face stiff monetary fines in addition to the possibility of losing landing privileges at U.S. airports.⁷

Europeans comprise the single largest group of international air travelers to the United States.⁸ To preserve this valuable source of revenue, European Union (EU) airlines were prepared to "do their best" to abide by the new ATSA regulations.⁹ Compliance, however, proved difficult because the ATSA's disclosure requirements squarely conflict with European Commission Directive 95/46 ("Data Protection Directive"), which regulates the collection and use of personal data.¹⁰

EU representatives recognized the importance of the U.S. antiterrorism legislation, but were nevertheless reluctant to permit European airlines to comply with the ATSA's disclosure requirements.¹¹ The European Commission embarked on negotiations with CBP officials to arrive at an agreement that would allow European airlines to comply with both the ATSA and with European law.¹² This process would prove to be a litigious and complex multiyear undertaking.

with Both European Union and United States Law, 14 *TRANSNAT'L L. & CONTEMP. PROBS.* 1137, 1139-40 (2005).

7. See 19 C.F.R. §§ 122.14(d)(5), 122.161 (2007) (setting forth the potential penalties airlines face for violations of aircraft regulations).

8. *Give Us Those Data*, *ECONOMIST*, June 3, 2006, at 47, 47 ("In 2004, 9.6 [million] EU citizens entered the United States by air, representing 48% of all foreign air travellers coming to America.").

9. M. Sefik Yuksel, Comm'r of the European Airline Ass'n, Address to European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs: Data Protection Since 11 September 2001: What Strategy for Europe (Mar. 25, 2003), available at <http://www.europarl.europa.eu/comparl/libe/elsj/events/hearings/20030325/yuksel.pdf>.

10. See Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive] (protecting the processing and collecting of individuals' personal data by member states); *Give Us Those Data*, *supra* note 8, at 47 (noting the conflict that European airlines face in meeting the U.S. requirements while at the same time obeying European privacy law).

11. See Letter from Stefano Rodotà, Chairman, Article 29 Working Party, to Jorge Salvador Hernández Mollar, Chairman, Comm. on Citizens' Freedoms and Rights, Justice & Home Affairs, European Parliament (Mar. 3, 2003), available at <http://www.statewatch.org/news/2003/mar/art29ch.pdf> [hereinafter Rodotà Letter] (underscoring the importance of counterterrorism legislation, but emphasizing the need to ensure compliance with European laws).

12. See Joint Statement, European Commission/U.S. Customs Talk on Passenger Name Record (PNR) Transmission (Feb. 17-18, 2003), available at http://ec.europa.eu/comm/external_relations/us/intro/pnr-joint03_1702.htm [hereinafter Joint Statement on PNR Transmission] (noting the shared intention of the European Commission and the CBP to negotiate a framework for European airlines to comply with both ATSA requirements and the Data Protection Directive); see also Rodotà Letter, *supra* note 11 (chronicling the multiyear negotiations between the Bureau of Customs and Border Protection (CBP) and the European Commission).

In May 2004, the European Commission and the CBP reached an agreement that purportedly satisfied the requirements of the Data Protection Directive and fulfilled the CBP's security needs.¹³ Members of the European Parliament, however, felt the agreement violated the terms of the Data Protection Directive and filed suit to have the agreement annulled.¹⁴ In May 2006, the European Court of Justice (ECJ) annulled the agreement.¹⁵ Less than a month later, however, the European Commission and the CBP devised a temporary arrangement permitting the exchange of PNR data.¹⁶ This provisional measure expired in July 2007, and has been supplanted by a relatively long-term agreement that governs the transfer of PNR data between the United States and European airlines.¹⁷

These protracted disputes illustrate a fundamental conflict in the way Europeans and Americans balance personal privacy and national security concerns. Part II of this Comment briefly examines and contrasts data privacy policies in the European Union and the United States. Part III traces the evolution of the conflict, beginning with an overview of several passenger surveillance regimes sanctioned by the ATSA, including Computer Assisted Passenger Prescreening System (CAPPS), CAPPS II, and Secure Flight. Additionally, Part III considers European responses to the expansive disclosure requirements and describes the dilemma airlines face given the conflicting obligations under EU and U.S. laws. Part IV analyzes the ECJ decision to annul the agreement between the European Union and the United States on narrow, technical grounds. Finally,

13. See Agreement Between the United States of America and the European Community on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004 O.J. (L 183) 83–85 [hereinafter 2004 Agreement] (documenting the bilateral agreement between the European Union and the United States regarding the transfer of PNR data).

14. Joined Cases C-317 & C-318/04, *Parliament v. Council*, 2006 E.C.R. I-4721.

15. *Id.* (annulling both the international agreement decision in C-317/04 and the adequacy decision in C-318/04).

16. See Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record (PNR) Data, 72 Fed. Reg. 348, 348 (Jan. 4, 2007) [hereinafter 2006 Agreement] (promulgating temporary rules governing the “transfer of [PNR] data by air carriers to the Department of Homeland Security”).

17. See Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), 2007 O.J. (L 204) 18–19, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0018:0025:EN:PDF> [hereinafter 2007 Agreement] (specifying that the agreement will be in effect for seven years “unless the parties mutually agree to replace it”).

Part V reflects on the conflict and considers the possibility that similar disagreements may arise between other nations. Drawing lessons from the dispute between the European Union and the United States, Part V proposes two methods to preempt or resolve such conflicts. First, it explores a model for developing a global, multilateral agreement for the transfer of PNR data. Second, it considers the merits of abandoning the use of PNR data altogether in passenger screening. This Comment concludes that while neither model offers an ideal strategy, a multilateral agreement is preferable.

II. APPROACHES TO SECURING DATA PRIVACY IN THE EUROPEAN UNION AND THE UNITED STATES

The concept of “privacy” is universally recognized as a significant and valuable collection of personal interests.¹⁸ The scope and interpretation of this “extremely broad concept” are debated and understood differently depending upon the context.¹⁹ As personal information becomes simpler to store, disseminate, and access, the importance of defining data privacy within the broader collection of privacy rights intensifies.²⁰ The European Union and the United States have markedly different approaches to securing their citizens’ personal data.²¹ Generally speaking, the European Union views privacy as a human right and protects this right through a “coherent and enforceable legal regime.”²² Data privacy protection in the United States, by contrast, is left to self-regulation by industries.²³ Accordingly, a description of the doctrinal underpinnings of these two different approaches provides the necessary background for understanding the significance of the PNR debate.

18. See, e.g., Universal Declaration of Human Rights, G.A. Res. 217A (III), art. 12, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 12, 1948) (“No one shall be subjected to arbitrary interference with his privacy . . .”).

19. See Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1093–94 (2002) (discussing various scholarly interpretations of the interests comprising “privacy”).

20. See Neil M. Richards, *The Information Privacy Law Project*, 94 GEO L.J. 1087, 1089–91 (2006) (observing that an “increasingly digitized society” has given rise to scholarship reexamining information privacy).

21. See Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 730–31 (2001) (observing that while the United States has left privacy regulation up to market forces, Europe treats privacy as a fundamental right and has enacted comprehensive legislation to safeguard data privacy).

22. Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT’L L.J. 2024, 2026–27 (1999).

23. See *id.* at 2025 (comparing the EU and U.S. approaches to data privacy).

Data privacy laws began to emerge in Europe during the 1970s, most notably in Germany, Sweden, and France.²⁴ As data transmission among European countries increased, the pressing need for a uniform set of rules for the use, storage, and transmission of data became evident.²⁵ In an attempt to foster a uniform set of European data protection laws, in 1980, the Organisation for Economic Co-operation and Development (OECD) established the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.²⁶ The following year, the Council of Europe established the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.²⁷ Both frameworks, however, were ultimately unsuccessful in articulating a unified European data protection policy.²⁸

The formation of the European Union in 1992 accelerated the development of uniform European data protection laws.²⁹ In 1995, the European Union enacted the Data Protection Directive, which requires member states to establish a regulatory framework governing all aspects of the collection, processing, and use of personal data.³⁰ The Data Protection Directive also has

24. See Patrick E. Cole, *New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws*, 17 N.Y.U. J. INT'L L. & POL. 893, 901–08 (1985) (chronicling the history of European data protection laws).

25. See Yohei Suda, *Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States*, 4 WASH. U. GLOBAL STUD. L. REV. 209, 215–16 (2005) (noting, for example, Sweden's refusal to recognize a British company's contract for manufacturing a magnetic data card because Sweden believed the British law did not offer sufficient data protection).

26. Organisation for Economic Co-operation and Development [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, at 423–27, O.E.C.D. Doc. C(80) 58 (Final) (Sept. 23, 1980), reprinted in 20 I.L.M. 422 (1981), available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (setting forth guidelines aimed at harmonizing privacy legislation among member countries).

27. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art. 1, Jan. 28, 1981, Europ. T.S. No. 108 (“The purpose of this convention is to secure . . . for every individual . . . respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (‘data protection’).”).

28. See Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 431–32 (1995) (observing that the OECD guidelines lack legal force and that a majority of nations have not ratified the Convention, and suggesting that these proposals failed because they were tolerant of significant variation in national data protection laws).

29. See *id.* at 432–33 (observing that political unification of the European Union intensified the need for a harmonized data protection standard).

30. Data Protection Directive, *supra* note 10, art. 6 (requiring that member states provide for fair and lawful processing of the data and collect data only for “specified, explicit and legitimate purposes”).

extraterritorial impact; Article 25 provides that data transfers to foreign countries are unlawful unless the recipient country ensures “adequate” protection of the data.³¹

Unlike the European Union’s relatively cohesive legislative approach to maintaining the security of citizens’ data, the United States employs a less structured, market-driven approach.³² The United States does not explicitly regulate the use of personal records, but instead enacts industry-specific “data protection” legislation on an as-needed basis.³³

Comparing Europe’s cohesive data protection framework with the U.S. market-driven approach highlights an underlying doctrinal difference: Europeans view data privacy as a fundamental right with few exceptions, whereas Americans balance the need to protect data privacy rights with the legitimate economic interests of collecting, storing, and trading personal information.³⁴ Deconstructing the events of the PNR debate in light of this distinction provides a richer understanding of each party’s motivation.

III. PENALTIES OR PROSECUTION?

The legislative response to the September 11 attacks was swift and comprehensive.³⁵ Among the first legislative measures enacted were those designed to protect the faltering airline industry and strengthen aviation security.³⁶ Before 2001, airlines and airports bore the primary responsibility for developing, enforcing, and funding aviation security measures.³⁷ Many

31. *Id.* art. 25.

32. *See* Pearce & Platten, *supra* note 22, at 2036–39 (describing the U.S. approach as “a patchwork of rules including constitutional, common, statutory, and regulatory laws”).

33. *See* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 471–72 (2000) (noting the reactive nature of U.S. data protection legislation exemplified by the Video Privacy Protection Act of 1988 and the Fair Credit Reporting Act).

34. *See* David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 954–56 (2003) (describing the conceptual underpinnings of the differing data protection policies).

35. Jay Mykytiuk, *Behind Closed Doors: Troubling Indications of Overbroad Secrecy in Anti-Terrorist Legislation in the United States and Canada*, 12 SW. J. L. & TRADE AM. 477, 477 (2006).

36. *See* Campbell, *supra* note 2, at 139 (examining aviation security legislation enacted in the wake of the terrorist attacks); MIGRATION POLICY INST., CHRONOLOGY OF EVENTS SINCE SEPTEMBER 11, 2001 RELATED TO IMMIGRATION AND NATIONAL SECURITY (2003), available at <http://www.migrationinformation.org/chronology.pdf> (listing and explaining key events that occurred after September 11).

37. *See* Kent C. Krause, *Putting the Transportation Security Administration in*

Americans felt the lack of comprehensive federal regulation of both airport and airline security contributed to the security failures that allowed the terrorist attacks to occur.³⁸ As a result, Congress enacted the ATSA, which created the TSA, a new federal agency responsible for administering federal control of security in all modes of transportation.³⁹ In addition to hiring and training thousands of security screeners,⁴⁰ the TSA began refining computer-screening systems in an effort to improve security in U.S. airports.⁴¹ This section first examines the development of the TSA's passenger screening systems and then analyzes the resulting conflicts with EU law.

A. *State of Passenger Screening*

By early 2003, the TSA had implemented several measures to fortify airport security, including federalizing passenger and baggage screening personnel and using advanced explosive detection systems to screen baggage.⁴² These measures, however, did not determine whether a particular passenger required additional screening.⁴³ Thus, the TSA announced its intention to address this shortcoming in a Privacy Act notice describing CAPPS II.⁴⁴

CAPPS II was designed to replace the then-existing CAPPS system.⁴⁵ CAPPS was used to select passengers for additional

Historical Context, 68 J. AIR L. & COM. 233, 234–35 (2003) (discussing security requirements of airplane and airport operators prior to September 11).

38. See, e.g., *Aviation Security and the Future of the Aviation Industry: Hearings Before the Subcomm. on Aviation of the H. Comm. on Transportation & Infrastructure*, 107th Cong. 371–73 (2001) (statement of John Meenan, Senior Vice President, Air Transport Association of America) (“[W]e believe it is time for finally putting in place a unified, Federal security system, utilizing all of the tools at the disposal of the United States government. This has been recommended repeatedly in the past and was a central recommendation of at least two Presidential Commissions.”).

39. Aviation and Transportation Security Act, Pub. L. No. 107-71, § 114, 115 Stat. 597, 597–604 (2001) (codified as amended in scattered sections of 5 U.S.C. and 49 U.S.C.).

40. See Krause, *supra* note 37, at 248 (observing that the TSA hired over 105,000 employees to fulfill its goals of securing the nation's airports).

41. See *id.* at 249–50 (discussing TSA's goals of improving computer-based passenger screening systems).

42. See Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 711–13 (2004) (observing the aviation industry's transformations since September 11, and detailing the measures put in place by the TSA to strengthen airport security).

43. See Linda L. Lane, *The Discoverability of Sensitive Security Information in Aviation Litigation*, 71 J. AIR L. & COM. 427, 428–29 (2006) (noting that computer screening systems were used to identify passengers for additional *baggage* screening, not *passenger* screening, prior to the September 11 terrorist attacks).

44. Privacy Act of 1974: System of Records, 68 Fed. Reg. 45,265 (Aug. 1, 2003).

45. Computer Assisted Passenger Pre-Screening System (CAPPS) is a computerized

2008] *THE PASSENGER NAME RECORD CONFLICT* 595

screening of checked luggage; it was not, however, used to identify passengers for questioning and personal searches.⁴⁶ The new CAPPS II proposal contemplated a comprehensive system to evaluate the security risk posed by each passenger and to recommend a commensurate security procedure.⁴⁷ The system was designed to provide an immediate assessment of a traveler's risk level by mining data contained in certain commercial and governmental databases.⁴⁸ As originally conceived, CAPPS II classified travelers into one of three groups upon check-in.⁴⁹ A "green" designation indicated that the passenger did not pose a security risk and was therefore eligible to board the airplane.⁵⁰ A "yellow" designation indicated that the passenger required additional screening.⁵¹ Depending on the results of the investigation, the passenger would be detained, denied the right to board, or permitted to board.⁵² Finally, if the system classified a passenger as a "red" security threat, the passenger would be detained or arrested.⁵³ The CAPPS II proposal met with significant criticism,⁵⁴ and the TSA cancelled development of the

screening program that analyzes passenger profiles to determine if a particular passenger poses a significant security risk that calls for heightened scrutiny. Lane, *supra* note 43, at 428–30. The profiles are formed by surveying data accumulated from a passenger's history of ticket purchases, including elements such as the passenger's address, method of payment, identity of travel companions, ticket purchase date, departure date, destination, origin, and whether the ticket was one-way or round-trip, and correlating it with information about terrorist activities. Stephen W. Dummer, Comment, *Secure Flight and Dataveillance, A New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It*, 75 MISS. L.J. 583, 587–88 (2006). Significantly, CAPPS did not scan any government or law enforcement databases. See Leigh A. Kite, Note, *Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?*, 61 WASH. & LEE L. REV. 1385, 1394 (2004) (listing the types of data used to identify high-risk passengers and noting the absence of government and law enforcement databases). Instead, CAPPS assembled and retrieved a security profile and created a threat index on the basis of the passenger's data. *Id.* If the threat index was sufficiently high, the passenger was subject to additional security checks. *Id.* Unfortunately, the architecture of the software was not disclosed before being replaced with CAPPS II, so the public may only speculate as to how the system functioned. See Dummer, *supra*, at 588.

46. See *supra* note 43 and accompanying text.

47. Rosenzweig, *supra* note 42, at 711–14.

48. *Id.* at 713–14.

49. Dummer, *supra* note 45, at 589.

50. *Id.* Such a passenger is considered "not untrustworthy" or has been identified as possessing "limited risk behavior, making them eligible to board the aircraft." *Id.*

51. *Id.* A passenger who is "potentially untrustworthy" or "may be a risk" will be classified as a "yellow" category passenger. *Id.*

52. *Id.*

53. *Id.* A passenger who is considered "untrustworthy" and therefore a risk to the aircraft will be classified as "red." *Id.*

54. See Kite, *supra* note 45, at 1390 & n.26 (noting that the program has "sparked widespread debate about its restrictions on civil liberties"); Sarah Kehaulani Goo, *Fliers*

system and introduced plans for a successor system, Secure Flight.⁵⁵ The TSA hoped Secure Flight would retain the security benefits of CAPPs II while allaying civil rights advocates' privacy concerns.⁵⁶ Unfortunately, Secure Flight has been plagued by many of the same criticisms as CAPPs II,⁵⁷ and TSA officials have pushed back Secure Flight's proposed implementation date to some time in 2008.⁵⁸

Whether Secure Flight's methodologies and data retention procedures sufficiently protect passenger data privacy rights is an ongoing debate, but clearly both Secure Flight and CAPPs II require electronic access to PNR records.⁵⁹ The ATSA explicitly gives the CBP the right to access PNR data from every airline arriving or departing from a U.S. airport.⁶⁰ The ATSA provides

to Be Rated for Risk Level, WASH. POST, Sept. 9, 2003, at A1 ("[CAPPs II] has sparked so much controversy among both liberal and conservative groups that the TSA has struggled to get it going.").

55. Dummer, *supra* note 45, at 590.

56. *See id.* at 590 (noting the TSA claim that Secure Flight "adresse[d] and incorporate[d]" the privacy concerns associated with CAPPs II); Kite, *supra* note 45, at 1391 ("[Civil liberties advocates] were concerned that the CAPPs II System treated every passenger like a terror suspect.").

57. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-374T, AVIATION SECURITY: SIGNIFICANT MANAGEMENT CHALLENGES MAY ADVERSELY AFFECT IMPLEMENTATION OF THE TRANSPORTATION SECURITY ADMINISTRATION'S SECURE FLIGHT PROGRAM (2006) (Testimony of Cathleen A. Berrick, Director of Homeland Security and Justice Issues, before the U.S. Senate Committee on Commerce, Science, and Transportation) (finding that Secure Flight suffers from security vulnerabilities and does not completely protect passenger data); *see also* Dummer, *supra* note 45, at 590 (alleging that Secure Flight merely eliminated the yellow classification from CAPPs II while retaining most of the flawed elements of the system).

58. *See Aviation Security: Reviewing the Recommendations of the 9/11 Commission, Hearing Before the Comm. on Commerce, Science, and Transp.*, 110th Cong. 18 (2007) (statement of Senator Mark Pryor) (noting that implementation work on Secure Flight is set to begin in 2008). Recently, information about yet another passenger profiling system, the Automated Targeting System (ATS), was disclosed. *See* Privacy Act of 1974; System of Records, 71 Fed. Reg. 64,543, 64,543-46 (Nov. 2, 2006) (describing the "Automated Targeting System," a security system designed to perform screening of "inbound and outbound cargo, travelers and conveyances" in the United States, which utilizes a broad array of PNR data including passenger name, address, phone number, e-mail address, number of bags, travel agent, and one-way ticket information). The Privacy Act notice disclosing ATS's passenger screening functions was unexpected and has stirred much controversy. *See, e.g.,* ACLU, *Comments of the American Civil Liberties Union to the Department of Homeland Security Regarding the Proposed Automated Targeting System*, Dec. 1, 2006, available at <http://www.aclu.org/privacy/gen/27593leg20061201.html> (decrying Department of Homeland Security's failure to provide for a reasonable period of time for public review and commentary of ATS's privacy implications and claiming the program "[w]ill put the government into the business of creating 'security ratings' for millions of its own citizens," "make judgments based on governmental databases that . . . are already riddled with errors," and "leave individuals without vital rights to review, correct or challenge [their] security ratings").

59. Dummer, *supra* note 45, at 609-10; Kite, *supra* note 45, at 1397.

60. *See* 49 U.S.C. § 44909(c) (Supp. IV 2004) (requiring that airlines submit the

2008] *THE PASSENGER NAME RECORD CONFLICT* 597

that if an airline refuses to make this information available, the airline's landing rights may be revoked or stiff monetary fines may be imposed.⁶¹ Unlike airline passengers, whose primary concerns with the ATSA's data disclosure requirements relate to the use and distribution of PNR data, airlines landing at airports in the United States are most troubled by the ATSA's broad punitive provisions.⁶² From the airlines' perspective, the importance of avoiding fines and preserving lucrative landing rights outweighs privacy concerns. Unfortunately, as the following section illustrates, conformance to the ATSA's disclosure requirements has been anything but straightforward.

B. The No-Win Dilemma of the European Airlines

Although the ATSA was designed to address the root causes of the security breaches that led to the September 11 terrorist attacks, it also presented European airlines with a challenging conundrum.⁶³ Airlines are bound not to disclose PNR data by the EU Data Protection Directive,⁶⁴ but face revocation of their landing rights and large monetary fines if they do not comply with the ATSA's PNR disclosure requirement.⁶⁵

The Data Protection Directive outlines a regulatory framework for implementing a "harmoniz[ed]" data protection regime across the European Union.⁶⁶ Specifically, the Data Protection Directive requires member states to ensure that personal data are lawfully processed, provides citizens with the

name, date of birth, sex, passport number and country of issuance, visa number or resident alien card, and any other information deemed necessary for security purposes to the CBP prior to landing at any U.S. airport).

61. See *supra* note 7 and accompanying text.

62. See Press Release, Ass'n of European Airlines, AEA 'Disappointed' at European Parliament Vote on Passenger Data Transfer to US (Apr. 1, 2004), available at <http://www.aea.be/AEAWebsite/DataFiles/Pr04-031.pdf> (noting that airlines are caught between comprehensive U.S. data turnover requirements and EU privacy protections and asserting that the airlines should not be burdened with additional costs associated with national security issues).

63. See *id.* (noting the difficulties of simultaneously complying with American data disclosure requirements and EU data protection laws).

64. See Data Protection Directive, *supra* note 10, art. 7 (listing the limited conditions under which personal data may be transferred between European member states).

65. See *supra* note 7 and accompanying text.

66. Flora J. Garcia, Comment, Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators, 15 *FORDHAM INTELL. PROP. MEDIA & ENT. L.J.* 1205, 1210 (2005). This directive, as contrasted with a regulation, was an "instruction" to member states to codify the directive's tenets into their respective laws to provide a uniform information policy across the European Union. *Id.* at 1211.

right to contest improper uses of data, and creates judicial remedies for unlawful processing of data.⁶⁷ Although the Data Protection Directive was primarily intended to unify data protection laws across Europe, it has had significant extraterritorial impact.⁶⁸ It requires that data sent to a foreign country be “adequately” protected.⁶⁹ That is, the Data Protective Directive prohibits data transfers to foreign countries whose data protection standards do not comport with its requirements.⁷⁰

In Europe, the ATSA’s PNR disclosure requirement immediately raised concerns as to whether the CBP’s data protection standards would be considered “adequate.” To the chagrin of European airlines, the Data Protection Directive’s Working Party⁷¹ opined that the ATSA did in fact conflict with the Data Protection Directive’s adequate protection requirement.⁷² This opinion was the first step in a lengthy and complex series of negotiations to clarify the airlines’ obligations under the conflicting legal requirements.

IV. NEGOTIATING A SOLUTION

A. *Joint Statement and Parliament’s Initial Objections*

Upon learning of the ATSA’s PNR disclosure requirement, European airlines that were obligated to comply with the Data Protection Directive requested relief from the competing EU and U.S. requirements.⁷³ In February 2003, CBP representatives met

67. Data Protection Directive, *supra* note 10, arts. 6, 14.

68. See Seth Hobby, Comment, *The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S. Position Has Progressed*, 1 INT’L L. & MGMT. REV. 155, 156–57 (2005) (describing the international reach of the Directive’s adequacy requirement to countries engaged in trade with EU member states).

69. Data Protection Directive, *supra* note 10, art. 25(2).

70. *Id.*

71. See *id.* art. 29 (establishing the Working Party, an independent advisory body on data protection and privacy, and authorizing the Party to examine member state laws adopted under the Directive and to give the European Commission an opinion on the level of protection of data in third countries).

72. See The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, 11647/02/EN, WP 66 (Oct. 24, 2002), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp66_en.pdf (analyzing the requirements of the Data Protection Directive vis-à-vis the U.S. PNR disclosure requirements and concluding that they are in conflict with one another).

73. See Int’l Air Transp. Ass’n, Comments of International Air Transportation Association in Respect to U.S. Customs Service Interim Rule on Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States (Aug. 26, 2002), available at http://www.epic.org/privacy/airtravel/iata_pnr_access1.pdf (voicing concern that the ATSA’s passenger data

2008] *THE PASSENGER NAME RECORD CONFLICT* 599

with members of the European Commission to craft a solution that would clarify the obligations of airlines bound by the competing U.S. and EU laws.⁷⁴ Following two days of negotiations, the European Union and the United States issued a joint statement announcing that a temporary solution had been reached (“Joint Statement”).⁷⁵ The Commission representatives pledged to ensure that EU data protection authorities would not sanction European airlines for complying with the ATSA’s disclosure requirements in exchange for CBP’s promise to fully

disclosure requirements, without significant modifications, will compel airlines landing or taking off from U.S. airports to violate data protection laws of the countries they serve).

74. See Joint Statement on PNR Transmission, *supra* note 12 (declaring intention of the European Union and the United States to reconcile U.S. disclosure requirements with the Data Protection Directive’s privacy standards). A full understanding of the principal EU governmental bodies and the EU law making process may be helpful. For an overview, see Michael J. McCormick, *A Primer on the European Union and Its Legal System*, ARMY LAW., Dec. 2002, available at http://www.loc.gov/rr/frd/Military_Law/pdf/12-2002.pdf.

The European Union’s legislative processes are complex, and the role that each institution plays differs based on the type of legislation under consideration. See McCormick, *supra*, at 4–5 (noting that the European Council of Ministers and the European Parliament share legislative duties). Institutional responsibilities were clarified in 1991 with the signing of the Maastricht Treaty. See Treaty on European Union, Feb. 7, 1992, 1992 O.J. (C 191) 1. The treaty balances power between EU institutions and individual member states by dividing EU policy into three distinct areas, which are often referred to as “pillars.” See Manuel Medina-Ortega, Comment, *A Constitution for an Enlarged Europe*, 32 GA. J. INT’L & COMP. L. 393, 409 (2004).

The first pillar, known as the “Community Pillar,” deals with economic policy and provides the “foundation for creating a common currency and central bank, managing a single monetary policy, and coordinating the many economic policies of the member states.” Claire R. Kelly, *Realist Theory and Real Constraints*, 44 VA. J. INT’L L. 545, 578–80 (2004). Community Pillar policy matters are subject to supranational regulation (i.e., the Community as a whole rather than individual member states govern these areas). See Laura Spitz, *At the Intersection of North American Free Trade and Same-Sex Marriage*, 9 UCLA J. INT’L L. & FOREIGN AFF. 163, 208 n.170 (2004) (providing a concise history of the development of the European Union). The second pillar—“Common Foreign and Security Policy”—encompasses matters related to foreign policy and military issues. Iliana Christodoulou-Varotsi, *Recent Developments in the EC Legal Framework on Ship-Source Pollution: The Ambivalence of the EC’s Penal Approach*, 33 TRANSP. L.J. 371, 374 n.22 (2006). Finally, the third pillar—“Police and Judicial Cooperation in Criminal Matters”—involves policies providing for cooperation between the member states to fight cross-border crime. *Id.*; see Medina-Ortega, *supra*, at 409 (noting that the second and third pillars of the European Union are designed to foster “intergovernmental cooperation”). Matters in the second and third pillars are subject to intergovernmental regulation with the member states retaining a significant level of control. See Medina-Ortega, *supra*, at 409 (“Decisions are adopted by the Council of Ministers with some assistance from the Commission and consultation of the Parliament.”). Each European law must be based upon a treaty provision, which is known as the “legal basis” for the law. Louis F. Del Duca, *Developing Global Transnational Harmonization Procedures for the Twenty-First Century: The Accelerating Pace of Common and Civil Law Convergence*, 42 TEX. INT’L L.J. 625, 633–34 (2007).

75. See Joint Statement on PNR Transmission, *supra* note 12 (outlining the temporary agreement on PNR data transfers).

disclose its use and dissemination of collected passenger data.⁷⁶ The Joint Statement was intended to serve as an interim compromise until the European Commission made a final decision on whether CBP's treatment of PNR data satisfied the Data Protection Directive's adequate protection requirement.⁷⁷ While the Joint Statement seemed to offer a useful compromise, many commentators and civil rights advocates questioned its legal authority as well as its partiality.⁷⁸

In addition to criticism by commentators, the Joint Statement incited discord between several EU institutions.⁷⁹ The European Parliament formalized its distaste for the Joint Statement when the Citizens' Rights and Freedoms, Justice and Home Affairs Committee (LIBE) adopted a resolution expressing harsh disapproval of the Joint Statement.⁸⁰ The resolution expressly criticized the Commission for failing to determine whether the CBP's request for PNR records was legitimately grounded in the ATSA's statutory language, for failing to secure a pledge from the CBP that future revisions of the U.S. law would explicitly respect the Data Protection Directive's requirements, and for the secretive and nonpublic nature of its proceedings.⁸¹ Furthermore, the resolution boldly stated that the Commission's agreement with the CBP lacked "any legal basis and could be interpreted as an indirect invitation to the national authorities to disregard Community law."⁸² The resolution

76. *See id.* (exempting certain confidential information from the requirements of the ATSA and providing for stiff penalties for any CBP personnel found to have disclosed sensitive information without authorization).

77. *See id.* (providing that the agreement was in place "[p]ending a Commission decision under Article 25.6 of the Data Protection Directive").

78. *See, e.g.*, Electronic Privacy Information Center, EU-US Airline Passenger Data Disclosure, http://www.epic.org/privacy/intl/passenger_data.html (last visited Apr. 8, 2008) (criticizing the agreement for providing the United States needlessly broad access to European PNR data).

79. *See EU Row Over Airline Passenger Data Transmission*, EDRI-GRAM (European Digital Rights, Brussels, Belg.), Mar. 12, 2003, available at <http://test.edri.org/issues/privacy/pnr?from=20> (noting that the Joint Statement caused a clash between the Commission and Parliament).

80. *See* European Parliament Resolution on Transfer of Personal Data by Airlines to the U.S. Immigration Service, 2004 O.J. (C 61) 381 [hereinafter European Parliament Resolution] (expressing regret for the "failure of the Commission [in its role] as guardian of the Treaties and Community law" with regard to the Joint Statement). This resolution did not have any binding effect; indeed, parliamentary resolutions are rarely binding but provide political leverage and are often influential in EU law making. *See* A.H. ROBERTSON, EUROPEAN INSTITUTIONS 44-45 (3d ed. 1973) (providing a description of the authority and effect of Parliamentary resolutions).

81. *See* European Parliament Resolution, *supra* note 80, at 381-84 (listing the shortcomings of the Commission's agreement with the CBP).

82. *Id.* The Resolution passed by a vote of 414 to 44, with 11 members abstaining.

2008] *THE PASSENGER NAME RECORD CONFLICT* 601

concluded that the agreement outlined in the Joint Statement was legally baseless and should, therefore, be suspended.⁸³

B. CBP Undertakings and EU Adequacy Finding

Despite already having secured a compromise with the European Commission (through the Joint Statement), the CBP responded to the Parliament's criticisms with a set of "Undertakings" that illustrated how PNR data would be used.⁸⁴ The CBP committed to implementing a system to filter "sensitive data" from PNR records.⁸⁵ Furthermore, the Undertakings provided that until the automated filters were in place, any sensitive data contained in a PNR record would not be used, would be deleted from any disclosure of the data, and would not be input into any automatic passenger prescreening systems.⁸⁶ Additionally, the use of any sensitive data would be subject to specific approval by a committee composed of the U.S. Deputy Commissioner of the CBP and the Department of Homeland Security Chief Privacy Officer.⁸⁷

In addition to promising the responsible and controlled use of PNR data, the Undertakings defined the manner and scope of CBP's access to the data.⁸⁸ The Undertakings provided that only data regarding persons traveling through, into, or out of the United States would be accessed.⁸⁹ Furthermore, data would be accessed using only "pull" technology until carriers implemented

See Parliament Vote on Transfer of Personal Data by Airlines to the U.S. Immigration Service, 2004 O.J. (C 61) 334. Partisanship and underlying institutional tensions may have played a role in the resolution's strong disapproval of the Commission's Joint Statement. *See EU Row Over Airline Data Transmission*, *supra* note 79 (observing that Parliament's Spanish rapporteur Jorge Salvador Hernández Mollar is "at war" with Commissioner Chris Patten).

83. *See* European Parliament Resolution, *supra* note 80, at 384 (calling for the suspension of the Joint Statement's provisions).

84. *See* UNDERTAKINGS OF THE UNITED STATES BUREAU OF CUSTOMS AND BORDER PROTECTION AND THE UNITED STATES TRANSPORTATION SECURITY ADMINISTRATION 2 (2003), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf [hereinafter UNDERTAKINGS] (limiting use of the PNR data to "detecting known and previously unknown persons with terrorist connections who are attempting to fly on commercial air transportation into, out of, through or within the United States").

85. *Id.* Sensitive data is defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning the health or sex life of the individual . . ." *Id.*

86. *Id.*

87. *Id.*

88. *See id.* at 3–4 (providing guidelines for CBP's direct access and storage of airlines' passenger reservation information).

89. *Id.* at 3.

systems capable of “push” transfers.⁹⁰ Under the pull scheme, the CBP agreed to abstain from accessing PNR data more than seventy-two hours prior to the flight’s departure.⁹¹

The Undertakings also included proposed terms for storing the PNR data.⁹² The CBP committed to limit online access to the data by its officers to seven days, after which the number of officers with access to the data would be further limited.⁹³ The PNR records would be stored for a period of seven years with strictly limited access.⁹⁴ Data that had not been manually accessed during the seven-year period would be destroyed.⁹⁵ Records that had been accessed would be retained for another eight years.⁹⁶

The CBP also committed to implementing certain system security standards to prevent data from being compromised.⁹⁷ Once CBP obtained the PNR data, it would be stored on an encrypted end-to-end closed intranet system, with a “read only” access connection controlled by the Customs Data Center.⁹⁸ Direct access to the data would be limited to certain TSA and CBP employees on a “need to know” basis.⁹⁹

Satisfied with the CBP’s proposals to safeguard the PNR data, the Commission began the legislative process of issuing an adequacy decision that would permanently permit European airlines to lawfully transfer PNR data to the CBP.¹⁰⁰ The

90. *Id.*; see also *Data Protection Recommendations on PNR*, EDRI-GRAM (European Digital Rights, Brussels, Belg.), July 2, 2003, available at <http://www.edri.org/edrigram/number12/pnr> (explaining that a push method of data transfer is one in which data is selected and transferred by airlines to the CBP, whereas a pull transfer method is one whereby the CBP has direct online access to airline and reservation systems databases).

91. UNDERTAKINGS, *supra* note 84, at 3–4. However, in the “unusual event” that the CBP becomes aware of a specific security risk, the passenger’s PNR information may be pulled more than seventy-two hours prior to take off in order “to ensure proper enforcement action may be taken when essential to prevent or combat a terrorist act or serious criminal offense.” *Id.*

92. *Id.* at 4.

93. *Id.*

94. See *id.* at 4 & n.7 (citing “employees assigned to the National Targeting Center” as the only group able to access the data during that seven-year period).

95. *Id.* at 4.

96. *Id.*

97. See *id.* at 4–5 (providing a detailed list of security standards governing storage and use of PNR data).

98. *Id.* at 4 (“[R]ead only’ access . . . mean[s] that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier’s reservation system.”).

99. *Id.*

100. Article 25 of the Data Protection Directive prohibits transfers of personal data to foreign nations unless the Commission determines that the intended recipient

2008] *THE PASSENGER NAME RECORD CONFLICT* 603

Commission's adequacy determinations are guided by a three-part process. First, the Commission issues a proposal declaring that the foreign nation's data protection standards meet the Data Protection Directive's standards. Second, the Article 29 Working Party analyzes whether the foreign nation's data protection scheme complies with the Directive. And third, the Article 31 Committee¹⁰¹ delivers an opinion declaring the data protection standards of the foreign country sufficient to meet the Directive's requirements.¹⁰² The Commission called upon the Article 29 Working Party to examine whether the CBP Undertakings met the adequate protection requirement of the Data Protection Directive.¹⁰³

Overall, the Working Party found that the CBP Undertakings were overbroad and inconsistent with the Data Protection Directive.¹⁰⁴ The opinion first criticized the fact that the Undertakings were not legally binding on U.S. authorities, and their language gave U.S. authorities broad latitude in how the PNR records could be used.¹⁰⁵ The Working Party also took issue with the Undertakings' approval of both push and pull data transfer technologies.¹⁰⁶ Only push technology, the Working Party stated, would be consistent with the Data Protection Directive's adequacy requirement.¹⁰⁷ Push technology would allow the European data controllers (the airlines) to be independent of U.S. data filtering and access methods, thus ensuring adequate protection under the Data Protection Directive.¹⁰⁸ The Working Party highlighted several other concerns with the Undertakings

possesses data protection policies and procedures that will guarantee adequate protection of the data. Data Protection Directive, *supra* note 10, art. 25.

101. *See id.* art. 31 (establishing a committee composed of representatives of the member states to oversee the Commission's adequacy determination process).

102. *See id.* arts. 25, 31 (listing the procedures that the Commission must follow to make an adequacy determination); Aneurin Hughes, *A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (CTH)*, 24 U.N.S. WALES L.J. 270, 271-72 (2001) (explaining the process for assessing adequacy).

103. *See* The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 4/2003 on the Level of Protection Ensured in the U.S. for the Transfer of Passengers' Data*, 2-3, 11070/03/EN, WP 78 (June 13, 2003), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_en.pdf (noting that the Commission requested the Working Party to review the Undertakings to form an adequacy opinion).

104. *See id.* at 3-10 (highlighting the protection of individuals' privacy rights as a fundamental concern).

105. *See id.* at 5-6 ("[T]he 'undertakings' create a very broad mandate for use and disclosure of the data 'as otherwise required by law'").

106. *Id.* at 6.

107. *Id.*

108. *Id.*

and concluded by noting that a multilateral, global solution might be best suited to resolving the adequacy dilemma.¹⁰⁹

C. Agreement and Parliament's Challenge

Despite the Working Party's adverse opinion of the Undertakings, Commissioner Frits Bolkestein was determined to craft a permanent solution to the airlines' conflicting data disclosure obligations.¹¹⁰ Addressing Parliament, Bolkestein acknowledged that the U.S. stance towards data protection was in conflict with the terms of the Data Protection Directive, but he argued that the threats of terrorist attacks and the importance of the EU–U.S. relationship justified a political compromise that deviated from EU privacy protections.¹¹¹ He proceeded to outline three potential courses of action. First, the European Union could continue to push the United States to strengthen its legal framework with regard to data privacy, so as to comply with the EU Data Protection Directive. Second, the European Union could enforce the Data Protection Directive and take action against airlines that did not comply. Or third, the European Union could negotiate a permanent, binding bilateral agreement with the United States, which could “bridge the gap between the two legal systems.”¹¹² He criticized and dismissed the first two options; the

109. See *id.* at 6–10 (expressing concern with the treatment of the time of data transfer, length of data retention, and enforcement mechanisms, amongst other concerns, and endorsing a multilateral framework to govern PNR data transfers).

110. See Frits Bolkestein, Member of the European Comm'n in Charge of the Internal Market and Taxation, Address to European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs: EU/U.S. Talks on Transfers of Airline Passengers' Personal Data 2 (Sept. 9, 2003), available at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/03/396&format=HTML&aged=0&language=EN&guiLanguage=en> (noting that while “there are no easy or ‘perfect’ solutions” the situation was “at best legally fragile [and] cannot be allowed to continue”). Bolkestein's cooperativeness was not reflective of the sentiments of many EU legislators. See, e.g., Letter from the Chairman to the Lord Filkin CBE, Parliamentary Under Secretary of State, Department for Constitutional Affairs (Feb. 12, 2004), available at <http://www.publications.parliament.uk/pa/ld200304/ldselect/ldcom/140/140we108.htm> (criticizing the Commission's hasty approval of the Undertakings and cautioning against a premature adequacy determination).

111. See Bolkestein, *supra* note 110, at 2 (commenting that the competing concerns of the United States and the European Union may be “irreconcilable,” but that a compromise is necessary).

112. See *id.* at 4 (outlining possible courses of action). The Data Protection Directive does not require an international agreement to permit international data transfers; a Commission adequacy determination is typically sufficient. Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 864 n.220 (2005). The CBP, however, wanted direct access to PNR records located in EU airline databases. *Id.* Article 7(c) of the Data Protection Directive permits data controllers (airlines) to provide such access to personal data only if “necessary for compliance with a legal obligation to which the controller is

2008] *THE PASSENGER NAME RECORD CONFLICT* 605

first could go on “indefinitely,” and the second could result in inconvenience for arriving EU airline passengers (“secondary inspections”) and economic consequences for EU airlines (possible fines and perhaps even having their landing rights withdrawn).¹¹³ He concluded that the most viable resolution to the conflict would be the negotiation of a bilateral agreement with the United States based on a Commission determination that the CBP data protection regime ensured adequate protection of the PNR data.¹¹⁴ Parliament expressed its disagreement with the Commissioner’s view by issuing a resolution harshly rebuking the Commission’s submissive approach to the PNR conflict.¹¹⁵

Undeterred, the Commission continued to take the necessary steps to enter into a permanent data transfer agreement with the CBP by submitting both a draft adequacy determination and a proposed agreement with the CBP to both the Council and Parliament.¹¹⁶ The Council promptly approved the agreement and the adequacy determination,¹¹⁷ but Parliament rejected the Commission’s adequacy determination on multiple grounds.¹¹⁸

subject.” Data Protection Directive, *supra* note 10, art. 7(c). A binding legal agreement with the CBP would serve as valid “legal act” that the airlines could rely upon to permit CBP access to PNR records without running afoul of Article 7(c). Bignami, *supra*, at 864 n.220.

113. Bolkestein, *supra* note 110, at 4.

114. *Id.* Bolkestein explained, however, that the Commission would pursue such an agreement “only with the clear support of the Parliament and Council.” *Id.* (emphasis omitted).

115. See Transmission of Personal Data by Airlines in the Case of Transatlantic Flights, EUR. PARL. DOC. P5_TA-PROV 0429 (2003), available at <http://www.statewatch.org/news/2003/oct/eppnrresol.pdf> (calling on the Commission to limit the transfer of data to U.S. authorities in accordance with the Working Party’s opinion).

116. See *Communication from the Commission to the Council and the Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, at 10–11, COM (2003) 826 final (Dec. 16, 2003), available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0826en01.pdf (outlining a detailed framework for action). When the Commission is granted the power to issue implementing measures pursuant to a European law (for example, the ability to make an adequacy determination under the Data Protection Directive), its authority is not absolute; the Commission must submit a draft of the implementing measure to both a committee of national representatives as well as the Parliament. Bignami, *supra* note 112, at 861. The committee must vote to approve the measure in order for it to take effect. *Id.* Parliament, however, generally does not have veto power. *Id.* Instead, Parliament merely has the authority to issue nonbinding resolutions approving or criticizing the measure, and the Commission is required to review the draft measure based on Parliament’s comments. *Id.*

117. Council Decision 2004/496, 2004 O.J. (L 183) 83 (approving a bilateral agreement between the European Union and the United States under which the CBP would be permitted to access PNR data).

118. See Resolution on the Draft Commission Decision Noting the Adequate Level of Protection Provided for Personal Data Contained in the Passenger Name Records (PNR) Transferred to the U.S. Bureau of Customs and Border Protection, EUR. PARL. DOC. P5_TA-PROV 0245 (2004), available at <http://www.statewatch.org/news/2004/mar/ep-pnr->

Parliament requested that the Commission withdraw the adequacy determination and warned the Commission that it would seek review with the ECJ if the determination were formally adopted.¹¹⁹

Notwithstanding Parliament's warning, the Commission, under its Article 25(6) authority, cemented the path to political agreement with the CBP by formalizing its adequacy determination.¹²⁰ The Commission also entered into a binding international agreement with the U.S. government; the agreement closely mirrored the original CBP Undertakings and included very few "concessions."¹²¹ The CBP agreed to reduce the length of storage of the PNR data to three and a half years, reserved the right to access thirty-four of the PNR data elements, and maintained the controversial pull transfer method.¹²² Privacy activists and members of Parliament were outraged by this apparently one-sided agreement.¹²³

D. *The ECJ Annulment*

A little more than a month after the announcement of the agreement, Parliament launched a legal challenge in the ECJ contesting the validity of both the Commission's adequacy finding and the international agreement.¹²⁴ Parliament's pleadings in these cases were closely aligned with its previous criticisms of the adequacy decision and the international

report.pdf (explaining Parliament's substantial concerns with the legality of the adequacy determination).

119. *See id.* (calling upon the Commission to retract the adequacy determination and reserving the right to appeal adoption of the adequacy determination to the European Court of Justice (ECJ) and to bring an action before the ECJ to verify the legality of any formal international agreement arising from the adequacy decision).

120. *See* Commission Decision 2004/535, 2004 O.J. (L 235) 11 [hereinafter Commission Decision 2004/535] (concluding that the CBP's data processing standards adequately protect passengers' PNR data).

121. 2004 Agreement, *supra* note 13; *see* Commission Decision 2004/535, *supra* note 120 (containing provisions the CBP agreed to follow under the adequacy determination).

122. 2004 Agreement, *supra* note 13; Commission Decision 2004/535, *supra* note 120.

123. *See, e.g., EU Agrees US PNR Deal*, STATEWATCH NEWS, <http://www.statewatch.org/news/2004/may/10eu-us-pnr-deal.htm> (last visited Jan. 28, 2008) (noting comments from Tony Bunyan, a Statewatch editor, complaining of the cavalier treatment of "personal data—including e-mail addresses and credit card details . . . [u]nder the guise of the 'war on terrorism'" and stating that the Agreement "breaks the rights and protections of the 1995 Directive" in its treatment of PNR data); *see also* Bignami, *supra* note 112, at 863–65 (describing Parliament's staunch opposition to the agreement and adequacy decision because of "numerous shortcomings").

124. *See* Joined Cases C-317 & C-318/04, *Parliament v. Council*, 2006 E.C.R. I-4721 (annulling both the adequacy determination and the agreement).

2008] *THE PASSENGER NAME RECORD CONFLICT* 607

agreement.¹²⁵ The central allegations were that the Commission's adequacy determination was an ultra vires act,¹²⁶ and that it breached fundamental rights¹²⁷ and principles of proportionality.¹²⁸ Parliament attacked the legality of the international agreement on the grounds that Article 95 was not an appropriate legal basis.¹²⁹ To the surprise and dismay of commentators and privacy activists,¹³⁰ the ECJ refused to

125. See Sharon Nolan, *EU Security Versus Civil Liberties: The Case of PNR Data Transfer* (2006), (unpublished report prepared for the BISA Annual Conference 2006, University of Cork), available at <http://www.bisa.ac.uk/2006/pps/nolan.pdf> (comparing Parliament's contentions in its prelitigation resolutions with the pleadings in the cases before the ECJ).

126. Parliament argued that the Commission's adoption of the adequacy decision was ultra vires because it exceeded the Commission's authority under article 3(2) of the Data Protection Directive. Application for Case C-318/04, *Parliament v. Commission*, 2004 O.J. (C 228) 32. Article 3(2) of the Directive provides that the Directive's protections extend only to data processing activities that occur within the scope of the first pillar. See Data Protection Directive, *supra* note 10, art. 3(2). A governmental institution's authority under a particular directive is determined by the policy area or legal basis upon which the directive was based. For example, if the directive's legal basis is Article 95, an EU institution may only act in accordance with its first pillar rights. See WALTER CAIRNS, *INTRODUCTION TO EUROPEAN LAW* 54–55 (2d ed. 2002). The first pillar encompasses economic matters, whereas foreign security policy and cross-border crime prevention are second and third pillar matters respectively. See *supra* note 74 and accompanying text (explaining the “pillar” framework in further detail). The Data Protection Directive is based on the first pillar. See Data Protection Directive, *supra* note 10, Preamble (noting that the Directive's legal basis is article 95 of the Treaty of the European Union); see also CAIRNS, *supra*, at 55 (noting that legislation passed under the authority of Article 95 is limited to first pillar policies). Therefore, the Commission's actions pursuant to the Directive are limited to first pillar areas. Parliament concluded that, because the data being transferred to the CBP was being used for public security (a Second Pillar subject matter), the Data Protection Directive was inapplicable. See Application for Case C-318/04, *Parliament v. Commission*, 2004 O.J. (C 228) 32.

127. In particular, Parliament argued that the adequacy decision interfered with the right to private life as guaranteed by article 8 of the European Convention on Human Rights. See Opinion of Advocate General Léger in *Parliament v. Council* (C-317/04) and (C-318/04), ¶¶ 193–96, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004C0317:EN:HTML> [hereinafter Advocate General's Opinion] (explaining the legal basis for Parliament's contentions).

128. Parliament contended the adequacy decision violated the principle of proportionality because it approved the collection and retention of an excessive number of data elements. See Application for Case C-318/04, *Parliament v. Commission*, 2004 O.J. (C 228) 32; see also Data Protection Directive, *supra* note 10, art. 6 (guaranteeing balanced use of personal data).

129. See Advocate General's Opinion, *supra* note 127, ¶¶ 116–18 (documenting Parliament's argument that Article 95 EC is the incorrect legal basis for the international agreement); see also *supra* notes 74 & 126 (explaining the legal basis for the Data Protection Directive).

130. See, e.g., Elspeth Guild & Evelien Brouwer, *The Political Life of Data: The ECJ Decision on the PNR Agreement Between the EU and the US*, CEPS POLICY BRIEF, July 2006, at 2–3, available at <http://www.libertysecurity.org/IMG/pdf/1363.pdf> (expressing astonishment at the ECJ's failure to entertain Parliament's human rights and proportionality arguments); *EU-US Agreement on Passenger Data Transfer Annulled*, EDRI-GRAM (European Digital Rights, Brussels, Belg.), June 7, 2006, available at

entertain any of Parliament's human rights or proportionality claims.¹³¹ Instead, in a brief opinion, the ECJ ruled that the adequacy decision was outside the scope of the Commission's authority and the international agreement was founded upon the incorrect legal basis.¹³²

The ECJ's conclusion that the Commission's adequacy decision was an ultra vires act was based on its interpretation of Article 3(2) of the Data Protection Directive.¹³³ The ECJ found that the plain language of Article 3(2) forecloses the Commission's authority to make an adequacy determination when the data processing activity concerns public security.¹³⁴ Article 3(2) of the Directive explicitly provides that its terms do not apply to data processing operations that involve "public security, defence, [and] State security."¹³⁵ The ECJ held that because data transfer requirements outlined in the Commission's adequacy determination were based on U.S. legislation designed to enhance security,¹³⁶ the adequacy determination violated the Article 3(2) limitation.¹³⁷ Thus, the Commission's adequacy determination was an ultra vires act, and the ECJ annulled it on those grounds.¹³⁸

The ECJ's discussion and disposal of the international agreement were similarly brief. The ECJ began by observing that the Data Protection Directive's legal basis is Article 95 EC and it is, therefore, a first pillar law.¹³⁹ Without much further discussion, the ECJ held that because the core purpose of the international agreement with the United States was to combat terrorism and enhance security, a first pillar law could not justify Community competence.¹⁴⁰ Therefore, the ECJ concluded that the international agreement was founded upon an untenable legal basis and ordered the annulment of the agreement.¹⁴¹

<http://www.edri.org/edrigram/number4.11/pnr> (noting that despite the fact that Parliament prevailed in the suit, the decision "should not be considered as a real victory of the European Parliament").

131. Joined Cases C-317 & C-318/04, *Parliament v. Council*, 2006 E.C.R. I-4721.

132. *Id.* ¶¶ 54–70. The Court held that the Commission's adequacy decision exceeded its scope of authority under article 3(2) of the Data Protection Directive and that the international agreement with the CBP was founded on the incorrect legal basis. *Id.*

133. *Id.* ¶¶ 54–60.

134. *Id.* ¶ 96 (describing the Article 3(2) scope limitation).

135. Data Protection Directive, *supra* note 10, art. 3(2).

136. *Parliament*, 2006 E.C.R. I-4721, ¶ 98.

137. *Id.* ¶ 106.

138. *Id.* ¶ 105.

139. *Id.* ¶ 101 & n.57.

140. *Id.* ¶¶ 67–70.

141. *Id.* ¶¶ 154–56.

2008] *THE PASSENGER NAME RECORD CONFLICT* 609

Perhaps the most significant consequence of the ECJ's decision is the dangerous loophole it may have created in EU data protection law.¹⁴² The ECJ's holding suggests that if data is being processed and transmitted for the purpose of "public security," the Data Protection Directive's safeguards are inapplicable.¹⁴³ Even if the holding is construed more narrowly, the opinion indisputably creates uncertainty whenever commercial entities collect personal data subsequently used for law enforcement purposes.¹⁴⁴ One example of such possible uncertainty is whether the Data Protective Directive is inapplicable to a credit card company that collects data as a part of its antifraud program.¹⁴⁵ If the gathering of such data were determined to be a "law enforcement" activity, the ECJ's ruling would apparently permit the data collector to use and transfer the data without any of the Data Protection Directive's safeguards.¹⁴⁶

The ruling weakens Parliament's institutional power in the PNR debate.¹⁴⁷ The ECJ's conclusion that the international agreement was ineffective only because it was founded on the incorrect legal basis permitted the Commission to salvage the agreement by simply making the minor, formalistic adjustment of changing the legal basis of the agreement.¹⁴⁸ Under the new agreement, properly based on the third pillar, Parliament is

142. See Press Release, Peter Hustinx, European Data Prot. Supervisor, PNR: EDPS First Reaction to the Court of Justice Judgment (May 30, 2006), available at <http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/06/8&format=HTML&age d=0&language=EN&guiLanguage=en> (commenting that the ECJ's finding that the Data Protection Directive is inapplicable in the law enforcement context creates a substantial void in EU data protection law).

143. See Guild & Brouwer, *supra* note 130, at 4 (noting, for example, that transmission of information to foreign countries or organizations from the Visa Information System would not be required to comply with the Data Protection Directive if the transfer was intended for police or security purposes).

144. See Edward C. Harris, *Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers*, 22 AM. U. INT'L L. REV. 745, 794 (2007) (observing that the ECJ's ruling creates significant uncertainty regarding the scope of the data protection directive).

145. See *id.* (raising various examples of uncertainty created by the Court's opinion).

146. See *id.*

147. See Guild & Brouwer, *supra* note 130, at 3 (stating that the decision's effect moves the PNR debate to the third pillar, where Parliament has "even less voice than in the first pillar").

148. See HENRIETTE TIELEMANS ET AL., *THE TRANSFER OF AIRLINE PASSENGER DATA TO THE U.S.: AN ANALYSIS OF THE ECJ DECISION (2006)*, reprinted in *BNA INTERNATIONAL WORLD DATA PROTECTION REPORT 5* (2006), available at <http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/Publication Attachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf>.

incompetent to legally challenge the agreement;¹⁴⁹ Parliament's power is reduced to filing a nonbinding resolution.

E. Recent Developments

The ECJ's decision to annul the adequacy determination and the agreement with the United States resurrected the European airlines' original dilemma: if they refused to disclose the PNR records, they would be subject to U.S. penalties, but if they complied with CBP demands, they risked prosecution under the Data Protection Directive.¹⁵⁰ Fortunately for the airlines, their uncertainty was short lived. In October 2006, following nine hours of negotiations, the Council of Ministers approved the Commission's request to change the legal basis of the PNR agreement from the first pillar to the third pillar.¹⁵¹ The negotiations gave rise to a temporary agreement consistent with the ECJ opinion. That agreement expired in July 2007, and has been replaced by a long-term accord that seeks to provide a stable framework for sharing of PNR data.¹⁵² The new agreement seems to have resolved the PNR debate between the European Union and United States, but privacy activists and slighted members of Parliament continue to challenge the agreement's legitimacy.¹⁵³

149. See Francesca Bignami, *European Court of Justice Strikes EU-US Agreement on PNR Data*, CONCURRING OPINIONS, May 31, 2006, http://www.concurringopinions.com/archives/2006/05/european_court.html (observing that Parliament is powerless to effect Community agreements based upon the second or third pillars); *The European Commission Dribbles the Parliament Again in the PNR Deal*, EDRI-GRAM (European Digital Rights, Brussels, Belg.), June 21, 2006, available at <http://www.edri.org/edriagram/number4.12/pnr> (observing that Parliament is powerless as a result of the ECJ's ruling).

150. See Bignami, *supra* note 149 (observing that the ECJ's opinion put airlines back into their original dilemma).

151. See Council Decision 2007/551, 2007 O.J. (L 204) 16 (EU), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00160017.pdf (invoking third pillar articles 24 and 38 of the Treaty of the European Union as the basis for the new agreement).

152. See 2007 Agreement, *supra* note 17 (providing for the periodic review of the agreement's implementation "with a view to mutually assuring the effective operation and privacy protection of their systems").

153. See generally, e.g., Remarks of Sophia in 't Veld, 2007 O.J. 41 (July 9, 2007), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070709+ITEMS+DOC+XML+V0//EN#creitem18> (contesting the validity and disputing the agreement's effectiveness at protecting citizens' data privacy rights).

V. TWO PROPOSED STRATEGIES: DEVELOPING A MULTILATERAL FRAMEWORK OR ABANDONMENT OF THE USE OF PNR DATA

The preceding analysis of the protracted negotiations between the European Union and the United States is a single illustration of what some commentators and legislators construe as a global conflict.¹⁵⁴ From this perspective, the costly and time-consuming events of the EU–U.S. PNR debate serve as a compelling reason for the establishment of a multilateral, global framework of standards governing the exchange of PNR data. Civil liberties advocates, on the other hand, have argued that the use of PNR records in passenger screening is ineffective, unnecessarily intrusive, and insecure.¹⁵⁵ These commentators further argue that the full-scale abandonment of PNR data in passenger screening is the best way to avoid future conflicts.¹⁵⁶ This section considers both proposals.

A. *A Multilateral Framework*

As the debate over the exchange of PNR data illustrates, variations in international privacy laws pose substantial challenges to airlines and governments bound by conflicting regulations.¹⁵⁷ The conflict between the European Union and the United States over the adequacy of data protection for PNR transfers exemplifies these challenges.¹⁵⁸ In the future, similar controversies may arise between different governments.¹⁵⁹ Data

154. See, e.g., *Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, at 9, COM (2003) 826 final (Dec. 16, 2003), available at http://ec.europa.eu/comm/external_relations/us/intro/apis_en.pdf [hereinafter *Communication from the Commission to the Council and the Parliament*] (describing the transfer of PNR data as a global rather than just a bilateral problem).

155. See, e.g., Letter from Elec. Frontier Found. to Privacy Office, U.S. Dep't of Homeland Sec. (Sept. 30, 2003), available at http://www EFF.org/Privacy/capsii/20030930_comments.php (arguing that screening systems that use PNR data are easily exploited and will be unsuccessful).

156. See, e.g., Letter from ACLU to Privacy Office, U.S. Dep't of Homeland Sec. (Sept. 20, 2003), available at <http://www.aclu.org/safefree/general/17681leg20030930.html> (calling for abandonment of the use of PNR data in passenger screening).

157. See generally *supra* Part III.B (describing the PNR conflict and the European airlines' compliance dilemma).

158. See Joel R. Reidenberg, *Opportunities and Obstacles for the Simplification of International Data Privacy Rules*, JUSLETTER, Oct. 3, 2005, at 2, available at <http://www.privacyconference2005.org/fileadmin/PDF/reidenberg.pdf> (describing difficulties encountered by multinational businesses attempting to comply with competing privacy regimes).

159. See *An International Framework for the Transfer of Passenger Name Record (PNR) Data* 3 (Int'l Civil Aviation Org., Working Paper No. 6325/04), available at <http://register.consilium.europa.eu/pdf/en/04/st06/st06325.en04.pdf> [hereinafter *PNR*

transfers from Canada, for example, require compliance with ten distinct data privacy obligations.¹⁶⁰ Canadian airlines flying to countries with expansive PNR disclosure requirements may face conflicting requirements. Advocates of a multilateral PNR agreement argue that the possibility of these types of controversies reoccurring around the world creates a strong incentive to form a harmonized, multilateral framework governing the transfer of PNR data.¹⁶¹

The EU–U.S. PNR agreement and the negotiations leading up to it serve as a useful background for proposing the structure and scope of a multilateral PNR agreement. During the course of the EU–U.S. PNR debate, the International Civil Aviation Organization (ICAO) submitted a working paper outlining a framework for a multilateral PNR agreement.¹⁶² The ICAO's proposed agreement offers a set of uniform data processing practices that makes PNR data available for law enforcement purposes while providing adequate protection of private data.¹⁶³ The ICAO's proposal begins by providing general guidelines regarding which data elements of a PNR should be included in a multilateral PNR transfer agreement.¹⁶⁴ Next, the proposal lists various data processing concerns that policy makers should consider when formulating a multilateral agreement.¹⁶⁵ Notably, several of the data processing elements mentioned in the ICAO proposal are similar to data processing requirements negotiated

Working Paper] (observing that more countries are likely to require the disclosure of PNR data and, as a result, conflicts are likely to occur).

160. See Todd A. Nova, Note, *The Future Face of the Worldwide Data Privacy Push as a Factor Affecting Wisconsin Business Dealing with Consumer Data*, 22 WIS. INT'L L.J. 769, 781 (2004) (explaining the ten requirements of Canada's Personal Privacy Protection and Electronic Documents Act: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance); see also David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 27 (1999) (examining data protection laws of over twenty countries and exploring Canada's Privacy Act).

161. See, e.g., *Communication from the Commission to the Council and the Parliament*, supra note 154, at 9; see also Anne Paylor, *Wanted: A Security Standard*, AIR TRANSPORT WORLD, June 2006, at 36, available at <http://www.atwonline.com/magazine/article.html?articleID=1634>.

162. See generally *PNR Working Paper*, supra note 159.

163. See *id.* at 3 (explaining the aims of the proposal).

164. See *id.* at 4 (proposing that a multilateral PNR data transfer agreement should be limited to those data elements strictly necessary for law enforcement purposes).

165. See *id.* at 4–5 (describing data processing elements that should be considered in a global PNR agreement, such as transparency, purpose limitation, storage, and redress mechanisms).

2008] *THE PASSENGER NAME RECORD CONFLICT* 613

by the CBP and the EU Commission.¹⁶⁶ Finally, the ICAO proposal recommends data transfer and data structure considerations that must be selected in a PNR agreement.¹⁶⁷ An agreement modeled on the ICAO's proposed framework conceivably could balance personal data privacy needs with governmental security requirements.

Although the notion of a cohesive multilateral framework governing the transfer of PNR data is enticing, several barriers complicate any realization of such a regulatory scheme. One obstacle to establishing a multilateral agreement on PNR data transfers is that "[p]rotection of the privacy of name-linked data is a[n] . . . issue characterized by sharp cross-national differences in basic beliefs and approaches."¹⁶⁸ Another factor that might hinder the creation of a multilateral solution to the PNR debate is that formalizing and ratifying multilateral accords is often a lengthy and disputatious process.¹⁶⁹ The length and intensity of the bilateral EU–U.S. debate over PNR data disclosures clearly illustrates the difficulty of striking even a bilateral balance. Creation of a multilateral agreement would be even more challenging because a greater number of government-access and citizen-privacy concerns would have to be addressed. Such an agreement might fail—as other multilateral privacy accords have failed in the past—by degenerating into an overly general and unenforceable agreement.¹⁷⁰

166. Compare *id.* (providing for additional safeguards for sensitive data, time and frequency limitations for accessing data, and redressing procedures for passengers with complaints concerning the treatment of their PNR data), with *UNDERTAKINGS*, *supra* note 84, at 2–9 (same).

167. See *PNR Working Paper*, *supra* note 159, at 5–6 (underscoring data transfer elements that a PRN agreement should include).

168. Stephen J. Kobrin, *Territoriality and the Governance of Cyberspace*, 32 J. INT'L BUS. STUD. 687, 699 (2001).

169. See ORAN R. YOUNG, *CREATING REGIMES: ARCTIC ACCORDS AND INTERNATIONAL GOVERNANCE* 4 (1998) (explaining the time consuming process of international treaty ratification).

170. See, e.g., Michael J. Gilligan & Nicole Simonelli, *International Multilateral Agreement Negotiations* (Oct. 13, 2006) (unpublished paper presented to the 2006 Shambaugh Conference), available at <http://www.saramitchell.org/GilliganSimonelli.pdf> (discussing various negotiation strategies used in reaching international multilateral agreements and the lengthy delays often experienced in reaching satisfactory agreements); see also HUNTON & WILLIAMS CTR. FOR INFO. POLICY LEADERSHIP, *GLOBAL PRIVACY PROTECTION FRAMEWORK* 1–3 (2003), http://www.hunton.com/files/tbl_s47Details/FileUpload265/1246/Global_Privacy_Protection_Framework.pdf (describing the inconsistent application of the OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* because of its breadth and generality).

B. Eliminate the Role of PNR Data in Passenger Screening

Eliminating the use of PNR data in the passenger screening process offers an attractive and simple resolution to the compliance problems posed by conflicting international privacy standards.¹⁷¹ Such a proposal is supported by at least two propositions: (1) the use of PNR data is ineffective at averting terrorist threats, and (2) the civil liberty costs of using PNR data are unjustifiably high. The following subsections consider each of these contentions.

1. *The Use of PNR Data Is Ineffective.* Numerous critics have argued the TSA's use of PNR data to prescreen passengers is ineffective.¹⁷² One line of reasoning is that members of terrorist cells can easily determine whether they will be automatically selected for additional screening during the planning stages of their terrorist attack.¹⁷³ Before executing any plan, terrorists can assess their threat rating by performing a "dry run." By boarding the flights they intend to hijack in advance of an attack, terrorists can determine whether their PNR data flags them for additional screening.¹⁷⁴ For the actual attack, any terrorist singled out during the dry run for additional screening can simply be replaced by one who was not singled out.

A would-be terrorist could also easily circumvent a screening system that relies on PNR data by posing as a low-risk passenger through the use of a stolen identity.¹⁷⁵ The CBP screening

171. See generally *supra* Part III.B (analyzing the difficulties faced by European airlines attempting to comply with conflicting data protection laws).

172. See, e.g., Electronic Privacy Information Center, Comments of the Electronic Privacy Information Center on Aviation Security Screening Records, at 13–14, <http://www.epic.org/privacy/airtravel/capps-comments.pdf> (last visited Apr. 11, 2008) (noting that CAPPS II is "error-prone [and] ineffective" due to the insufficiency of data correction procedures); Laura W. Murphy, Director, ACLU Washington Legislative Office, Remarks at the National Press Club, Washington, D.C.: America, Land of the Watched: CAPPS II and the Dangers of Unchecked Surveillance (Aug. 25, 2003), available at <http://www.aclu.org/safefree/general/16768prs20030825.html> (insisting that through identity theft, one can easily avoid detection by PNR-based screening systems).

173. See Samidh Chakrabarti & Aaron Strauss, Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System, (May 16, 2002) (unpublished student paper, Mass. Inst. Of Tech.), available at <http://swissnet.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm> (arguing that PNR-based passenger screening systems may be easily defeated using the "dry run" methodology explained here).

174. See *id.* (explaining how utilizing dry runs to identify an unflagged passenger might frustrate the goals of a PNR-based computer screening system).

175. See Jill D. Rhodes, *CAPPS II: Red Light, Green Light, or 'Mother, May I?'*, J. HOMELAND SEC., Mar. 2004, <http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=107> (asserting that the ease of identity theft may permit terrorists to escape detection by PNR-based screening systems). See generally Stephen W.

2008] *THE PASSENGER NAME RECORD CONFLICT* 615

systems relying on PNR data would be unable to detect terrorists using false passports. The PNR information linked to the false passport would not raise any red flags, and the terrorist would bypass PNR-related security measures. According to the Government Accountability Office, identity theft is the most common and successful way passport fraud is perpetrated.¹⁷⁶ A 2003 Federal Trade Commission survey found that approximately 10 million consumers in the United States were victims of identity theft in the year preceding the study.¹⁷⁷ Given the prevalence of identity theft, the determined terrorist might easily obtain a false passport and defeat the PNR screening system.¹⁷⁸

2. *Civil Liberties Concerns.* Even if screening systems were developed in a way to safeguard against the practice of dry runs and the use of stolen identities, the further contention that these systems unreasonably infringe upon civil liberties merits consideration.¹⁷⁹

One argument is that PNR-based screening systems violate constitutional protections against unreasonable searches and seizures. Stephen Dummer has analogized the use of PNR data to screen passengers with “sending the police to thoroughly review every available personal document in your home, without a warrant, every time you wanted to drive your car.”¹⁸⁰ Searches, however, do not violate the Fourth Amendment unless they are unreasonable.¹⁸¹ Furthermore, the Supreme Court has hinted that in public places, such as airports, a greater level of intrusion may be required to deem a search unreasonable as compared to

Dummer, *False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft*, 11 J. TECH. L. & POL'Y 259, 279–83 (2006) (arguing that genuine concern about the accuracy of passenger screening systems exists due to identity theft).

176. See U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-853T, STATE DEPARTMENT: IMPROVEMENTS NEEDED TO STRENGTHEN U.S. PASSPORT FRAUD DETECTION EFFORTS 6 (2005), available at <http://www.gao.gov/new.items/d05853t.pdf> (Statement of Jesse T. Ford, Director, International Affairs and Trade) (observing that, in 2004, 69% of all detected passport frauds were committed using stolen identities).

177. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 4 (2003), <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

178. See Rhodes, *supra* note 175.

179. See, e.g., Russell Hardin, *Civil Liberties in the Era of Mass Terrorism*, 8 ETHICS 77, 79 (2004) (commenting on the need for an even-handed approach to combating terrorism).

180. Dummer, *supra* note 45, at 595.

181. See *id.* at 595–96 (citing JAMES J. TOMKOVICZ & WELSH S. WHITE, CRIMINAL PROCEDURE: CONSTITUTIONAL CONSTRAINTS UPON INVESTIGATION AND PROOF (4th ed. 2001)).

private places.¹⁸² Dummer contends, however, that the Court's reasoning is outdated and needs to be reconsidered in light of the technological advances in screening capabilities.¹⁸³

In addition to constitutional criticisms, privacy advocates fear the emergence of a surveillance state in which the government maintains life-long travel dossiers on each citizen.¹⁸⁴ Systems based on PNR data, such as CAPPS II or Secure Flight,¹⁸⁵ may easily be used to create and store travel profiles on every traveler that comes through a U.S. airport, regardless of the individual's alleged "threat level."¹⁸⁶ Commentators argue such a regime restricts innocent citizens' decisional privacy interests¹⁸⁷ and information privacy interests.¹⁸⁸ Indeed, privacy activists' fears were realized in late 2003 when Jet Blue turned over 5 million passenger records to Torch Concepts, a TSA contractor, for their use in testing the CAPPS II system.¹⁸⁹ In addition to this PNR data, Torch purchased vast quantities of consumer demographic information from Acxiom, a commercial data aggregator.¹⁹⁰ Torch then matched the PNR information

182. See *Katz v. United States*, 389 U.S. 347, 350–52 (1967) (distinguishing one's expectation of privacy during a telephone conversation in a telephone booth from a communication made publicly).

183. See Dummer, *supra* note 45, at 596–98 (asserting that the Supreme Court's holding in *Katz* should be revisited to provide guidance on the level of privacy one can expect in public places such as airports, with the knowledge that automated screening systems are a possibility).

184. See Edward Hasbrouck, *Travel Privacy*, <http://hasbrouck.org/articles/PHR2004-travelprivacy.pdf> (last visited Apr. 11, 2008) (detailing the collection and retention of PNR data infringing the legitimate privacy interests of innocent travelers).

185. See *supra* Part III.A (describing CAPPS II and Secure Flight).

186. See Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 792 (2006) (observing that privacy concerns have not been adequately considered in the implementation of computer-based screening systems storing personal travel data).

187. See Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. BALT. L. REV. 1, 13 (2006) (defining autonomy privacy interests or decisional privacy as the "right to make personal choices free from government interference or restriction").

188. See Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 324 (2004) (defining information privacy interests as being "concerned with 'precluding the dissemination or misuse of sensitive and confidential information'" (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 654 (Cal. 1994))).

189. Anita Ramasastry, *Airline Passenger Profiling Based on Private Sector Data: Why It Raises Serious Privacy Concerns*, FINDLAW'S WRIT, Oct. 1, 2003, available at <http://writ.news.findlaw.com/ramasastry/20031001.html>; see also Editorial, *Betraying One's Passengers*, N.Y. TIMES, Sept. 23, 2003, at A30 (declaring Jet Blue's disclosure as "one of the most serious betrayals of consumers' privacy rights by an American business").

190. Ramasastry, *supra* note 189. The disclosed Acxiom information "included gender; whether the passenger owned or rented his or her residence, and how long he or she had lived there; economic status, including income; number of children; Social Security number; occupation; and vehicle information." *Id.*

2008] *THE PASSENGER NAME RECORD CONFLICT* 617

with the commercial data and classified the travelers into three categories: “(1) Young Middle Income Home Owners with Short Length-of-Residence; (2) Older Upper Income Home Owners with Longer Length-of-Residence; and (3) travelers with ‘anomalous records.’”¹⁹¹ Privacy advocates were enraged by the study and expressed concern that it was an unwarranted intrusion into the private lives of innocent citizens.¹⁹²

3. *Adequate Safeguards Exist.* While privacy activists present a compelling case for eliminating the use of PNR data in the passenger screening process, perhaps the argument is overbroad.¹⁹³ One criticism of the pro-privacy position is that it is too quick to label the use of PNR data as a reduction in privacy.¹⁹⁴ Instead, PNR-based screening calls for “trade-offs in different types of privacy.”¹⁹⁵ Computerized passenger screening systems substitute electronic privacy intrusions for the physical privacy intrusions of airport body searches.¹⁹⁶ Thus, PNR-based screening systems do not necessarily reduce the level of privacy; they simply exchange one type of privacy for another.¹⁹⁷

The contention that computerized screening systems are ineffective because they may easily be defeated is also widely critiqued.¹⁹⁸ Critics have argued that a security system should not be abandoned simply because it is theoretically possible to defeat its protections.¹⁹⁹ The notion that a dry run defeats a computerized screening system is also easily dismissed. The dry run tactic would be completely ineffective and unreliable if the computerized screening system were supplemented with random

191. *Id.*

192. Letter from Lisa Dean, Elec. Frontier Found., to Don Young and James Oberstar, Chairman & Ranking Member, House Comm. on Transp. & Infrastructure (Feb. 17, 2004), available at http://w2.eff.org/Privacy/capsii/coalition_letter.php (requesting congressional hearings into the governmental usage of the privately released PNR data provided by Jet Blue).

193. See, e.g., Rosenzweig, *supra* note 42, at 663–65 (noting that the emerging “anti-anti-terror” movement overestimates the privacy intrusion incurred by the use of technology to combat terrorism).

194. See *id.* at 715 (asserting that civil liberty advocates fail to consider the important increases in physical privacy that PNR screening provides).

195. *Id.*

196. *Id.*

197. *Id.*

198. See, e.g., K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, 67 n.285 (2003) (asserting arguments that PNR-based systems may be easily defeated should not be taken seriously as these arguments are countered by the additional costs and risks PNR-based systems impose on terrorists).

199. See *id.* (noting that this privacy advocates’ argument is as absurd as arguing that locks should not be used because skilled burglars may pick them).

physical searches.²⁰⁰ Simply because an unflagged terrorist is able to pass through the system without being investigated based on his PNR record, there is no guarantee that he would be able to avoid a random search.

Finally, privacy activists disregard the fact that technological safeguards can protect against the abuse or misuse of disclosed PNR data.²⁰¹ For example, anonymization techniques offer methods for private data to be analyzed without compromising privacy.²⁰² A promising anonymization technology known as a “one-way hash function” permits multiple data holders to cooperate in evaluating data while fully protecting privacy.²⁰³ The technique applies a data encryption algorithm to scramble a given piece of data into an unrecognizable string of letters and numbers, known as a “hash value.”²⁰⁴ If two data holders apply the same algorithm to the same set of data, the resulting scrambled strings are identical.²⁰⁵ This technique allows determination of a particular set of information appearing on distinct lists without the parties sharing the lists between themselves.²⁰⁶ If implemented correctly, it would be possible for airlines to disclose hashed PNR data to a trusted third party who would compare the airline list to a similarly hashed list of government terrorism suspects, turning over only matching records to the government.²⁰⁷ In this way, the government could

200. See Taipale, *supra* note 198, at 67 n.285 (noting that the “dry run” theory should be taken into account when computerized systems are being developed to incorporate “adaptive . . . learning” techniques, but does not justify abandoning such systems).

201. See generally JAMES X. DEMPSEY & PAUL ROSENZWEIG, CENTER FOR DEMOCRACY & TECHNOLOGY, TECHNOLOGIES THAT CAN PROTECT PRIVACY AS INFORMATION IS SHARED TO COMBAT TERRORISM 1–2 (2004), <http://www.cdt.org/security/usapatriot/20040526technologies.pdf> (claiming that the debate over the use of technology in counterterrorism centers on “unsubstantiated claims of utility or non-specific fears of abuse” that do not adequately analyze opportunities for the inclusion of protective measure).

202. See Stewart Baker et al., Anonymization, Data-Matching and Privacy: A Case Study 4 (Dec. 2003), <http://www.stepto.com/publications/279d.pdf> (explaining how anonymization procedures could distort identifying information in passenger lists, yet still allow systems to compare them against lists of terrorism suspects thereby preventing disclosure of the true identity of most passengers).

203. See *id.* (describing cryptographic techniques that can be used for anonymization).

204. See *id.* (explaining the “one-way hash function” technique).

205. See DEMPSEY & ROSENZWEIG, *supra* note 201, at 8 (describing the general process and benefits of the hashing technique).

206. See Baker et al., *supra* note 202, at 4 (applying hash function technology to the PNR context, particularly between the European Union and United States where the transfer of personal data is even more restrictive).

207. See *id.* (asserting that the inclusion of an independent third party to perform the matching process would enhance personal privacy by eliminating the availability of the original data).

monitor suspected terrorists while preserving the privacy of innocent travelers.²⁰⁸

VI. AN IMPERFECT SOLUTION

Although both solutions described above have merit, neither is perfect. The vital importance of maintaining national security, coupled with the various privacy safeguards protecting PNR data from misuse, indicate that abandoning computerized screening is not the right solution. Rather, a multilateral agreement is preferable. Even though establishing multilateral agreements can be extremely time consuming and may come with the risk of being written so vaguely that they are effectively unenforceable, multilateral agreements on PNR data transfer would not compromise national security concerns in the way that abandoning the PNR regime altogether would.

VII. CONCLUSION

The difficulty of striking the proper balance between personal privacy interests and the government's need to preserve national security has been a contentious issue in the post-September 11 world. In the immediate aftermath of the attacks, the United States adopted legislation designed to bolster national security.²⁰⁹ Laws such as the Patriot Act bartered privacy interests for the promise of increased security.²¹⁰ 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.²¹¹

The EU–U.S. debate over PNR data shows the pendulum has not yet swung fully in the direction of privacy preservation. The Commission's negotiations with the CBP admittedly were aimed at a “political” solution rather than to uphold the principles of the Data Protection Directive.²¹² Furthermore, the

208. See *id.* (stating that only when there is a match would information be turned over to the U.S. government).

209. See Block, *supra* note 1, at 471–78 (discussing post-September 11 legislation).

210. See Kevin Bankston & Megan E. Gray, *Government Surveillance and Data Privacy Issues: Foundations and Developments*, PRIVACY & INFO L. REP., Apr. 2003, at 1, 3 (asserting that the Patriot Act was hastily enacted and did not provide sufficient protections for civil liberties).

211. See *id.* at 10 (considering the notion of assigning a dollar value to lost privacy rights when making security-related budget decisions as a means to balance the benefit of increased security against the Constitutional cost).

212. See Bolkestein, *supra* note 110, at 4 (emphasizing the need for a bilateral

ECJ's procedural disposition of Parliament's challenge not only limited Parliament's future rights to challenge the agreement with CBP, but also dramatically reduced the scope of the Data Protection Directive. Arguably, Parliament was the only institution truly insistent upon ensuring that the agreement with the United States reflected the data protection goals of the Data Protection Directive. Of course, such a characterization of the conflict is at least somewhat exaggerated because many factors other than the preservation of data security protections contributed to the outcome. For example, the Commission was forced to weigh the potentially disastrous economic consequences the airlines faced if an agreement with the CBP was not rapidly reached. In any case, the debate has served as a useful barometer for assessing the state of balance between personal privacy rights and governmental security needs.

Although in some respects the EU-U.S. PNR conflict illustrates that the prevailing socio-political climate tolerates trading privacy rights for promises of increased national security, it simultaneously demonstrates that arriving at a cross-cultural agreement that strikes precisely the appropriate balance between both interests is an extremely complex undertaking. The lengthy and multifaceted negotiations serve as a warning of what may be in store for pairs of governments with varying data protection standards and inconsistent PNR transfer requirements. This Comment has evaluated two methods of avoiding a costly conflict of this nature in the future and concludes that, despite significant shortcomings, a multilateral agreement on the transfer of PNR data should be implemented.

Irfan Tukdi

agreement between the European Union and the United States, rather than risk the consequences resulting from the enforcement of the Data Protection Directive).