

**COMMENT: THE EUROPEAN COURT OF
JUSTICE’S DECISION TO ANNUL THE
AGREEMENT BETWEEN THE UNITED STATES
AND EUROPEAN COMMUNITY REGARDING THE
TRANSFER OF PERSONAL NAME RECORD DATA,
ITS EFFECTS, AND RECOMMENDATIONS FOR A
NEW SOLUTION**

*Vanessa Serrano**

I.	INTRODUCTION	454
II.	THE EUROPEAN UNION’S LAWS AND UNITED STATES REGULATIONS THAT IMPACTED THE AGREEMENT AND ITS ANNULMENT	455
A.	<i>Directive 95/46/EC—European Privacy Directive</i>	456
B.	<i>Article 8 of the European Convention for the Protection of Human Rights</i>	456
C.	<i>Treaty Establishing the European Community</i>	457
1.	Article 94 & Article 95.....	457
2.	Article 251.....	457
3.	Article 253.....	458
4.	Article 300.....	458
D.	<i>Aviation and Transportation Act of 2001 (ATSA)</i>	459
E.	<i>Code of Federal Regulations—Customs Duties</i>	459
III.	THE ROAD TO CONFLICT: OPINIONS, AGREEMENTS AND RECOMMENDATIONS.....	460
A.	<i>Data Protection Working Party’s Opinion 2/2004</i>	460
B.	<i>European Commission Decision 2004/535/EC</i>	461
C.	<i>European Council Decision 2004/496/EC</i>	462
D.	<i>Agreement between the European Community and the United States</i>	462
E.	<i>Case C-318/04 and Case C-317/04</i>	463
F.	<i>Opinion of Advocate General Leger delivered on November 22, 2005</i>	464
IV.	RULING BY THE EUROPEAN COURT OF JUSTICE	466
A.	<i>Holding of Case C-318/04</i>	466

* Vanessa M. Serrano is currently a third year law student at Nova Southeastern University’s Shepard Broad Law Center, where she is a member of the ILSA Journal of International and Comparative Law. She received a Bachelor of Science in Business Administration in Marketing from the University of Central Florida in 2002. The author would like to take this opportunity to thank her parents for their unconditional love and support.

B. <i>Holding of Case C-317/04</i>	467
V. ANALYSIS—THE FLAWS IN THE AGREEMENT AND RECOMMENDATIONS FOR POSSIBLE SOLUTIONS THAT WILL APPEASE BOTH SIDES	468
VI. CONCLUSION	469
VII. UPDATE.....	470

I. INTRODUCTION

As a result of the September 11th terrorist attacks on the United States, the U.S. government implemented new laws and regulations for international air carriers landing in U.S. airports. These regulations require that the air carriers provide the Bureau of Customs and Border Protection (CBP) with information regarding the passengers on the flight within fifteen minutes of departure.¹ Air carriers that refuse to comply with the regulations can be denied landing rights² or charged fines.³ These new regulations have forced air carriers outside of the United States to examine their policies and the passenger information that is required by CBP.

The European Union (EU) entered into an agreement with the United States on May 28, 2004 in order to transfer the passenger name record (PNR) data to CBP on all flights from the EU's Member States⁴ to the United States.⁵ The agreement was based on the European Council and Parliament's Directive 95/46/EC (European Privacy Directive) that limits the transfer of data to third countries in order to protect the privacy rights of citizens of the EU's Member States.⁶ The European Council (Council) relied on this agreement and on several articles found in the Treaty

1. 19 C.F.R. § 122.49a(b)(2)(i) (2006).

2. 19 C.F.R. § 122.14(d)(5) (2006).

3. 19 C.F.R. § 122.161 (2006).

4. *See generally* 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, U.S.-Eur., May 28, 2004, 2004 O.J. (L 183) 84, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf [hereinafter Agreement]; European Union, Delegation of the European Commission to the USA, <http://www.eurunion.org/states/offices.htm> (last visited Oct. 6, 2006). The EU's Member States include: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Spain, Slovakia, Slovenia, Sweden and the United Kingdom.

5. *Id.*

6. *See generally* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Oct. 24, 1995, 1995 O.J. (L 281) 31, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [hereinafter European Privacy Directive].

Establishing the European Community (EC Treaty)⁷ to form the legal basis for their actions. Shortly after the agreement was finalized, Parliament filed two suits in the European Court of Justice (ECJ).

Parliament's first case petitioned the ECJ to annul the European Commission's (Commission) decision that declared that the United States provided an "adequate level of protection" for the PNR data that is transferred to the CBP.⁸ The second case petitioned the ECJ to annul the Council's decision to approve the agreement between the European Community and the United States.⁹ The pleas in each of the cases contested the legal basis for the decisions, the content of the agreement and decision of adequacy, and other privacy factors that were of concern to the Parliament.¹⁰ The ECJ combined the two cases and held that both decisions would be annulled on May 30, 2006.¹¹

This article will discuss the ECJs decision and possible changes that will be required in order to continue flights from the EUs Member States into the United States. Part I will discuss the various laws in the EU and United States that resulted in the need for an agreement and the subsequent annulment of the agreement. Part II will discuss the various opinions that have been released on the subject and the decisions that led to Parliament's suits. Part III will discuss the ECJs ruling and their reasoning for annulling the decisions. Part IV will analyze the ECJs decision and recommend possible solutions to future agreements between the United States and the EU.

II. THE EUROPEAN UNION'S LAWS AND UNITED STATES REGULATIONS THAT IMPACTED THE AGREEMENT AND ITS ANNULMENT

Parliament filed the two suits in the ECJ because of the differences between the EUs privacy laws and the new travel regulations in the United States. The following are brief explanations of each of the applicable laws and regulations.

7. See generally Consolidated Version of the Treaty Establishing the European Community, Dec. 24, 2002, 2002 O.J. (C 325) 33, available at http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E_EN.pdf [hereinafter EC Treaty].

8. Application for Case C-318/04, Parliament v. Council, 2004 O.J. (C 228) 32 (2004), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/c_228/c_22820040911en00320033.pdf.

9. Application for Case C-317/04, Parliament v. Comm'n, 2004 O.J. (C 228) 31, 32 (2004), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/c_228/c_22820040911en00310032.pdf.

10. EC Treaty, *supra* note 7; Application for Case C-318/04, *supra* note 8.

11. Joined Cases C-318/04 & C-317/04, Parliament v. Council & Parliament v. Comm'n, 2006 E.C.R. ¶ 75 available at <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-317/04> [hereinafter *Joined Cases C-318/04 & C-317/04*].

A. *Directive 95/46/EC—European Privacy Directive*

In 1995, Parliament and Council released a directive that controlled how an individual's personal information could be processed and shared by Member States.¹² The object of the European Privacy Directive was to protect the fundamental rights and freedoms of the EU's citizens, specifically the right to privacy.¹³ Generally speaking, the European Privacy Directive was created to ensure that individuals' privacy rights would not be infringed by the processing of personal data by Member States.

The European Privacy Directive lists specific guidelines for transferring data within the Member States and to countries outside of the EU. Article 25 states that all third countries must provide an "adequate level of protection" for the data in order to receive it from any Member State of the EU.¹⁴ Factors that are considered to determine adequacy include the type of data, the purpose of the transfer, the amount of time the data will be held, and the privacy laws of the third country.¹⁵ Any country that does not meet the level of adequacy required by the European Privacy Directive will not be eligible to receive the data transfers. The European Privacy Directive permits the Commission to enter into negotiations with any third country that does not meet the adequacy standards in order to ensure protection of the privacy rights of the individuals.¹⁶ This policy was the basis for the agreement between the United States and the European Community.

B. *Article 8 of the European Convention for the Protection of Human Rights*

The European Privacy Directive was created to enforce the EU's privacy laws, namely Article 8 of the European Convention for the Protection of Human Rights.¹⁷ This law declares that every individual has a right to privacy in their private and family lives, place of dwelling, and all personal communications.¹⁸ Article 8 prohibits law enforcement from

12. European Privacy Directive, *supra* note 6.

13. *Id.* at art. 1.

14. *Id.* at art. 25.

15. *Id.*

16. *Id.*

17. See generally Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Nov. 4, 1950, 213 U.N.T.S. 222, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm> [hereinafter Convention for the Protection of Human Rights and Fundamental Freedoms].

18. *Id.*

interfering with an individual's privacy rights, unless the interference is required to protect "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."¹⁹ The EU's privacy laws protect the rights of individuals, but also recognize the need to infringe on those rights in order to protect the security and well-being of the Member States.²⁰

C. *Treaty Establishing the European Community*

1. Article 94 & Article 95

Articles 94 and 95 of the EC Treaty set out the method for creating directives to be followed by the Member States. Article 94 requires that the European Community submit the proposed directives to the Council.²¹ In order to enact the proposed directive, there must be a unanimous approval by the Council. In addition, both Parliament and the Economic and Social Committee must be consulted.²²

Article 95 gives the Council the authority to adopt new policies that protect the internal market.²³ Council must consult the Economic and Social Committee and must follow the procedures that are required in Article 251 of the EC Treaty.²⁴ The term "internal market" is not defined by the EC Treaty.

2. Article 251

Article 251 specifies the procedure for enacting new laws in the EU.²⁵ The Commission makes recommendations for the new law to the Council and Parliament.²⁶ Parliament is then given an opportunity to submit an opinion to the Council regarding possible amendments to the Commission's proposal.²⁷ Once Parliament submits the opinion, the Council may either enact the law with Parliament's recommendations, enact the law if

19. *Id.*

20. *See generally* Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 17, at art. 8.

21. EC Treaty, *supra* note 7, at art. 94.

22. *Id.*

23. EC Treaty, *supra* note 7, at art. 95.

24. *Id.* at art. 95, 251.

25. EC Treaty, *supra* note 7, at art. 251.

26. *Id.*

27. *Id.*

Parliament did not make any suggested amendments, or respond to Parliament with a modified version of the law.²⁸ If Council responds with a modified version of the proposed law, Parliament then has three months to approve the law, reject it by a majority vote of Parliament, or respond with new amendments for the Council to review.²⁹

3. Article 253

Article 253 of the EC Treaty requires that all decisions by Parliament and the EU list the specific reasons and rationale that led to the decision.³⁰ The Council and Commission must follow the same procedure when adopting new laws.³¹ This requirement ensures that all actions by the governing bodies of the EU have sufficient explanation and reasoning that can be referred to if there is a conflict.

4. Article 300

Article 300 discusses the process of entering into international agreements. Similar to the process of creating new laws as described in Article 251, the Commission makes recommendations, which are then approved by a majority of the Council.³² International agreements that entail creating associations among the Member States require unanimous approval by the Council.³³

The Council must submit the Commission's proposed agreement to Parliament so that they have an opportunity to respond with an opinion.³⁴ If the situation is an emergency, Council and Parliament may agree upon a time limit for Parliament to submit their comments.³⁵ If the proposed agreement amends an existing law, the Council must go a step further and have the agreement approved by Parliament rather than simply allowing them the opportunity to submit an opinion.³⁶ All international agreements that are negotiated by the Commission are binding on all of the Member States of the EU.³⁷

28. *Id.*

29. *Id.*

30. EC Treaty, *supra* note 7, at art. 253.

31. *Id.*

32. *Id.* at art. 300.

33. *Id.* at art. 310.

34. *Id.* at art. 300.

35. EC Treaty, *supra* note 7, at art. 300.

36. *Id.*

37. *Id.*

D. Aviation and Transportation Act of 2001 (ATSA)

The United States enacted the Aviation and Transportation Act (ATSA) in 2001, following the attacks on the World Trade Center and Pentagon earlier that year.³⁸ ATSA created a new government position called the Under Secretary of Transportation for Security (Under Secretary).³⁹ The Under Secretary was given the authority to manage security information by using Federal databases to identify individuals on flights who may pose a threat to national security.⁴⁰ The Under Secretary was also given the authority to create procedures to identify and notify the appropriate agencies of individuals who may pose a threat.⁴¹ One recommended procedure included requiring air carriers to provide passenger lists in order to help identify possible terrorist threats.⁴²

ATSA requires that all foreign air carriers provide passenger manifests for the passengers and crew members aboard flights into the United States.⁴³ It recommends information that the manifests should provide, including passenger names, date of birth, gender, passport information, and other information that the Under Secretary considered necessary to ensure safety.⁴⁴ This new law signified an important change for air carriers that travel to and through the United States. It also prompted other new regulations that provide specific instructions for the air carriers to follow, which are detailed in the Code of Federal Regulations.

E. Code of Federal Regulations—Customs Duties

New regulations in the Code of Federal Regulations (CFR) were then created to give Customs specific rules and regulations to abide by. These regulations state that all air carriers flying into the United States from international origins must provide an electronic passenger manifest to CBP for all passengers onboard the airplane within fifteen minutes of departure to the United States.⁴⁵ The CFR provides a lengthy list of required information that must be included in the electronic manifest, including the passenger's name, date of birth, gender, citizenship, country of residence,

38. Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified as amended in scattered sections of 49 U.S.C.A.).

39. 49 U.S.C.A. § 114(b)(1) (2000 & Supp. 2001).

40. 49 U.S.C.A. § 114(h)(1) (2000 & Supp. 2001).

41. 49 U.S.C.A. § 114(h)(2) (2000 & Supp. 2001).

42. 49 U.S.C.A. § 114(h)(4) (2000 & Supp. 2001).

43. 49 U.S.C.A. § 44909(c)(1) (2000 & Supp. 2001).

44. 49 U.S.C.A. § 44909(c)(2) (2000 & Supp. 2001).

45. 19 C.F.R. § 122.49a(b) (2006).

and address while in the United States.⁴⁶ The regulation stipulates that CBP may share the manifest with other Federal agencies to protect national security, and may share the information as authorized by United States law.⁴⁷

The new regulations give Customs the authority to deny or withdraw the landing rights of air carriers flying into the United States. Landing rights may be withdrawn if the air carriers do not comply with CBPs instructions.⁴⁸ The CFR also grants CBP the right to impose a 5000 dollar civil penalty to air carriers that do not comply with CBPs regulations.⁴⁹ These laws pose a problem for countries who do not wish to provide CBP with the electronic passenger manifests. They especially pose a problem for countries such as the Member States of the EU, who have strict privacy laws regarding the transfer of this type of information.

III. THE ROAD TO CONFLICT: OPINIONS, AGREEMENTS AND RECOMMENDATIONS

A. *Data Protection Working Party's Opinion 2/2004*

The Data Protection Working Party released an opinion on January 29, 2004 regarding concerns about the agreement that the Commission was negotiating with the United States.⁵⁰ These concerns included: the purpose of the data transfers; the amount of information being transferred; the amount of time the information would be stored; the transfer of sensitive data; the rights of passengers to know that the information was being transferred and the right to correct the data, if necessary; the level of commitments by U.S. authorities; the transfer of the information to other government agencies; and the preferred "push" method of transferring the

46. 19 C.F.R. § 122.49a(b)(3) (2006). The following information is required according to the Code of Federal Regulations: Full name; DOB; Gender; Citizenship; Country of residence; Status on board the aircraft; Travel document (passport, alien registration card); Passport number, if passport is required; Passport country of issuance; Passport expiration date; Alien registration number, where applicable; Address while in the US (not required for US citizens, lawful permanent residents, or people in transit to a location outside the US); Passenger Name Record locator, if available; International Air Transport Association (IATA) code of foreign port/place where transportation to the US began; IATA code of port/place of first arrival; IATA code of final foreign port/place of destination for in-transit passengers; Airline carrier code; Flight number; and Date of aircraft arrival. *Id.*

47. 19 C.F.R. § 122.49a(e) (2006).

48. 19 C.F.R. § 122.14(d)(5).

49. 19 C.F.R. § 122.161.

50. See generally Opinion 2/2004 of the Working Party on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, WP 87 (Jan. 29, 2004), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf [hereinafter Working Party Opinion 2/2004].

information to CBP rather than allowing them to extract the information themselves.⁵¹ Similar issues had been raised in previous opinions by the Data Protection Working Party. Despite this opinion, the Commission continued with their negotiations with the United States. Many of these concerns were later raised by Parliament in their petitions to annul the decisions.

B. European Commission Decision 2004/535/EC

On May 14, 2004, the Commission officially declared that the United States provided an adequate level of protection for the PNR data that would be transferred to the CBP under the new agreement.⁵² This decision was necessary in order to create an agreement to transfer PNR data to the United States. The Commission based their conclusion on the European Privacy Directive's requirements regarding data transfers to third countries. The decision stated that it was effective for three and a half years and would be monitored on a regular basis to ensure that the adequacy levels remained sufficient in accordance with the European Privacy Directive.⁵³

Parliament was concerned with this decision because the privacy laws in the United States are substantially different from the laws of the EU. The United States gives the government a considerable amount of leeway in permitting the transfer of data between agencies and other organizations. Overall, the United States does not offer the same amount of protection to an individual's personal information as compared to the EUs privacy laws.

Ultimately, the Commission and United States agreed on thirty-four items of data that would be transmitted to CBP in the electronic passenger manifests. These items include:

PNR record locator code; date of reservation; date(s) of intended travel; name; other names on PNR; address; all forms of payment information; billing address; contact telephone numbers; all travel itinerary for specific PNR; frequent flyer information (limited to miles flown and address(es); travel agency; travel agent; code share PNR information; travel status of passenger; split/dividend PNR information; e-mail address; ticketing field information; general remarks; ticket number; seat number; date of ticket issuance; no show history; bag tag numbers; no show information; OSI information; SSI/SSR information; received from information; all historical changes to PNR; number of travelers on PNR; seat information; one-way tickets; any

51. *Id.* at 13.

52. Commission Decision 2004/535/EC, 2004 O.J. (L 235) 11, 13 (2004), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf.

53. *Id.* at 14.

collected APIS (Advanced Passenger Information System) information; and ATFQ (Automatic Ticketing Fare Quote) fields.⁵⁴

According to the Commission's decision, the purpose of the transmission of the PNR data was preventing international terrorist acts and organized crime.⁵⁵ It was agreed that the PNR data would be stored for up to three and a half years by CBP.⁵⁶ The data would be available to the passengers by request and the passengers would be notified that the data was being transmitted to CBP.⁵⁷ The data could then potentially be transferred to other United States government agencies for security purposes and solely on a "case-by-case basis".⁵⁸ Many of these factors were items of concern in opinions released by the Data Protection Working Party.

C. *European Council Decision 2004/496/EC*

Three days after the Commission released their decision, the Council published a decision approving the proposed agreement between the United States and the European Community.⁵⁹ The Council acknowledged that they had given the Commission permission to negotiate with the United States and noted that Parliament had not submitted an opinion regarding the agreement within the agreed time frame.⁶⁰ The Council had established a deadline for Parliament to respond to the proposed agreement. They failed to submit the opinion on time, so the Council approved the decision, relying on Article 300 of the EC Treaty. The agreement was later signed by the President of the Council.

D. *Agreement between the European Community and the United States*

The final agreement between the European Community and United States was signed on May 28, 2004.⁶¹ The agreement recognized the privacy rights of the EU citizens and acknowledged the European Privacy

54. *Id.* at 22.

55. *Id.* at 15.

56. *Id.* at 14.

57. Commission Decision 2004/535/EC, *supra* note 52, at 19.

58. *Id.* at 18.

59. See generally Council Decision 2004/496/EC, 2004 O.J. (L 183) 83 (2004), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00830083.pdf.

60. Council Decision 2004/496/EC, *supra* note 59.

61. See generally Agreement, *supra* note 4.

Directive.⁶² It referred to paragraph 6 of Article 25 of the European Privacy Directive and the Commission's decision on adequacy dated May 14, 2004 as its authority.⁶³ According to the document, CBP would access the PNR data directly from the air carriers' reservation/departure systems, until a system was developed that would allow them to send the electronic manifests directly to CBP.⁶⁴ The data would be processed in accordance with U.S. law and the terms of the agreement.⁶⁵ The United States agreed to cooperate if the EU decides to implement a similar program to collect PNR data from air carriers in the future.⁶⁶ Each party retained the right to cancel the agreement at any time.⁶⁷

E. Case C-318/04 and Case C-317/04

As expected, a few months after the agreement was finalized two cases were filed in the ECJ by Parliament. The first case was Case C-318/04, in which Parliament filed a case against the Commission.⁶⁸ Parliament petitioned the court to annul the Commission's decision 2004/535/EC, which declared that the United States provided an adequate level of protection for the PNR data.⁶⁹ Parliament's petition was based on the following four pleas:

- 1) The Commission exceeded their powers by issuing the decision;
- 2) The decision breached the fundamental principles of the European Privacy Directive;
- 3) The decision was an infringement of fundamental rights;
- 4) The decision breached the principle of proportionality because it permitted the transfer of an excessive amount of information to CBP.⁷⁰

The second case was Case C-317/04 in which Parliament petitioned the ECJ to annul the Council's decision of May 17, 2004, which approved the international agreement.⁷¹ Parliament's petition was based on the following six pleas:

62. Agreement, *supra* note 4, at 84.

63. *Id.*

64. *Id.*

65. *Id.* at 85.

66. *Id.*

67. Agreement, *supra* note 4, at 84.

68. Application for Case C-318/04, *supra* note 8.

69. *Id.* at 32.

70. *Id.*

71. Application for Case C-317/04, *supra* note 9, at 32.

- 1) Incorrect choice of Article 95 of the EC Treaty⁷² as the legal basis for the agreement;
- 2) The agreement could only be concluded after the assent of the Parliament had been obtained;
- 3) The agreement infringed fundamental rights, including the right to protection of personal data and unjustifiable interference with private life;
- 4) Infringement of the principle of proportionality because of the excessive amount of passenger data being transferred and the disproportionate length of time that the data would be stored by CBP;
- 5) Lack of a sufficient statement of reasons for a measure having such specific characteristics;
- 6) Infringement of the principle of cooperation in good faith provided for in Article 10 of the EC Treaty.⁷³

F. Opinion of Advocate General Leger delivered on November 22, 2005

Philip Leger, the Advocate General of the ECJ, delivered an opinion on November 22, 2005 regarding Parliament's pending cases.⁷⁴ His analysis of Case C-318/04 concluded that the adequacy decision should be annulled because the European Privacy Directive does not apply to information being transferred for purposes of national security.⁷⁵ That being the case, the European Privacy Directive could not be the basis for the agreement and the Commission lacked the authority to negotiate the agreement.⁷⁶

Advocate General Leger's opinion stated that both of Parliament's cases should be considered together since they shared several similar pleas and content.⁷⁷ His analysis of Case C-317/04 recommended the annulment of Council's approval of the agreement in Council's Decision 2004/496/EC.⁷⁸ Regarding Parliament's first plea, Advocate General Leger concluded that Article 95 of the EC Treaty was not the appropriate legal

72. See EC Treaty, *supra* note 7, at art. 95.

73. Application for Case C-317/04, *supra* note 9, at 32.

74. See generally Case C-317/04, *Parliament v. Council*, 2005 O.J. 1, available at <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Rechercher&alldocs=alldocs&docj=docj&docop=docop&docor=docor&docjo=docjo&numaff=C-317/04&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100> [hereinafter *Case C-317/04*].

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

basis for the Council's decision.⁷⁹ Article 95 requires that international agreements regarding matters that affect the EU's internal market must be approved by a majority of the Council.⁸⁰ Advocate General Leger opined that the transfer of data to the United States did not affect the "establishment and functioning of the internal market" and that therefore, Article 95 was not the correct legal basis.⁸¹

The second plea in Case C-317/04 declared that the Council lacked authority to approve the agreement because the agreement amended the European Privacy Directive.⁸² According to Article 300 of the EC Treaty, any agreement that amends an existing law must be approved by Parliament.⁸³ Advocate General Leger found that this plea was unsubstantiated because the agreement did not amend the European Privacy Directive, therefore Parliament's approval was not required.⁸⁴

The third and fourth pleas claimed that the agreement infringed upon the individual's right to the protection of personal data and breached the principle of proportionality. Advocate General Leger also found these claims to be false.⁸⁵ He reasoned that interference into an individual's private life can only be allowed if it is done according to the law in order to achieve a legitimate goal and is necessary for the well-being of society.⁸⁶ He found that the process of transferring the data according to the agreement did not violate any of the privacy laws of the EU and that preventing terrorism and organized crime was a valid objective.⁸⁷ He also noted that the 34 items of passenger data that would be transferred in the electronic manifests was not an excessive amount of data and did not breach the principle of proportionality.⁸⁸

Parliament's fifth plea alleged that the Council did not sufficiently state the reasons behind its decision. Advocate General Leger opined that the Council's decision was adequate because it contained an explanation of the Council's process in making the decision.⁸⁹ According to Advocate

79. Case C-317/04, *supra* note 74.

80. EC Treaty, *supra* note 7, at art. 95.

81. Case C-317/04, *supra* note 74.

82. *Id.*

83. EC Treaty, *supra* note 7, at art. 300.

84. Case C-317/04, *supra* note 74.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. Case C-317/04, *supra* note 74.

General Leger, the decision followed the procedure required by the EC Treaty and cited proper authority to the EC Treaty.⁹⁰

Lastly, Parliament plead that the Council breached the duty of good faith that is required by Article 10 of the EC Treaty.⁹¹ Parliament's argument is that the agreement was finalized without their approval and before they were able to submit their opinion.⁹² The Council argues that Parliament did not present their opinion to Council in a timely manner and that the Council followed proper procedure.⁹³ Advocate General Leger agreed that the necessary procedures were followed and that the Council did not violate its duty of good faith.⁹⁴

Overall, Advocate General Leger recommended the annulment of both decisions. Although many of Parliament's pleas were unfounded in his opinion, both the Commission and Council lacked the proper legal basis for their decisions. Many of his recommendations appeared in the ECJs ultimate decision, which was delivered earlier this year.

IV. RULING BY THE EUROPEAN COURT OF JUSTICE

The ECJ released its final opinion on May 30, 2006.⁹⁵ Following Advocate General Leger's recommendation⁹⁶, Parliament's cases were combined into one opinion. The following is an explanation of each of the holdings and the ECJs rationale.

A. *Holding of Case C-318/04*

The ECJ annulled the Commission's decision that declared that the United States provided an adequate level of protection for the PNR data.⁹⁷ The decision was annulled based on Parliament's first plea that the Commission exceeded their powers by issuing the decision.⁹⁸ The Commission's legal basis for negotiating the agreement and issuing the adequacy decision was the European Privacy Directive. The ECJ ruled that

90. *Id.*

91. EC Treaty, *supra* note 7, at art. 10. Article 10's good faith requirement mandates that the Member States and bodies of the European Community avoid any activities that could interfere with the objectives of the EC Treaty. Parliament was trying to argue that Council was not acting in accordance with the good faith requirement by proceeding without having received their opinion on the agreement.

92. Case C-317/04, *supra* note 74.

93. *Id.*

94. *Id.*

95. See Joined Cases C-318/04 & C-317/04, *supra* note 11.

96. See Case C-317/04, *supra* note 74.

97. Joined Cases C-318/04 & C-317/04, *supra* note 11.

98. *Id.* ¶ 60.

the agreement between the United States and the European Community did not fall within the scope of the European Privacy Directive because it concerned a matter of national security.⁹⁹ Article 3 of the European Privacy Directive specifically states that issues of national security are not protected by the directive; therefore it was not the proper legal basis for the Commission's actions and decision.¹⁰⁰

The remaining three pleas were not addressed by Parliament because the initial plea was enough to invalidate the Commission's decision.¹⁰¹ The fact that this decision was annulled consequently affected Parliament's case C-317/04 because it invalidated the European Privacy Directive as the Commission's authority to enter into negotiations with the United States.

B. *Holding of Case C-317/04*

The ECJ then annulled the Council's decision to approve the agreement between the European Community and United States.¹⁰² It found that Article 95 of the EC Treaty was not the appropriate legal basis for the agreement.¹⁰³ The court held that the agreement was related to the processing of passenger data for the protection of national security, which is excluded from the scope of the European Privacy Directive.¹⁰⁴ In addition, Article 95 permits the Council to enter into agreements whose function is to protect the internal market of the EU.¹⁰⁵ According to the ECJ, the agreement did not affect the internal market and was not authorized under the European Privacy Directive.

Once again, the ECJ did not examine Parliament's other five pleas. The Council's decision was annulled solely on the fact that the agreement lacked the appropriate legal basis under Article 95.¹⁰⁶ While deciding to annul both decisions, the ECJ agreed to continue the effectiveness of the agreement until September 30, 2006 in order to give the Council time to make new arrangements with the United States.¹⁰⁷

99. *Id.* ¶ 59.

100. European Privacy Directive, *supra* note 7, at art. 3.

101. Joined Cases C-318/04 & C-317/04, *supra* note 11, ¶ 61.

102. *Id.* ¶ 70.

103. *Id.* ¶ 67.

104. *Id.* ¶ 59.

105. EC Treaty, *supra* note 7, at art. 95.

106. Joined Cases C-318/04 & C-317/04, *supra* note 11, ¶ 69.

107. *Id.* ¶ 74.

V. ANALYSIS—THE FLAWS IN THE AGREEMENT AND
RECOMMENDATIONS FOR POSSIBLE SOLUTIONS THAT
WILL APPEASE BOTH SIDES

The agreement remains in place today and will expire at the end of September. In the meantime, the Commission has gone back to the drawing board in order to draft an agreement that will placate Parliament and conform to U.S. regulations. The Commission recently released a statement saying that they are currently working on a “legally sound framework”¹⁰⁸ in order to continue transferring the PNR data from the air carriers in the Member States to the United States. The Commission has a limited amount of time to fix a potentially very large problem.

The interruption of the agreement at the end of September could have a significant impact on travel to the United States from the Member States of the EU. All air carriers traveling from the EU's Member States to the United States could face fines and be denied landing rights if they do not provide the CBP with the required PNR data. This could lead to increased competition from air carriers in other countries who are complying with the U.S. regulations. This would impact the economies of the Member States by decreasing the income generated by air travel to the United States. It not only affects flights to the United States, but also affects flights stopping in the United States on their way to other destinations.

It is important to note that both cases were voided based on technicalities, rather than violations of the EU's privacy laws. Parliament's ultimate concern was the privacy rights of the individuals, yet the ECJ did not address any privacy issues in its decision. The Parliament and Data Protection Working Party had several concerns regarding the agreement that were not addressed, including the method of transferring the information to the United States, the amount of time the United States was storing the information, and the amount of information being transmitted. They also argued that the agreement went against the privacy rights of the European citizens established by the EU. The fact that the European Privacy Directive regarding data transfers does not apply to PNR data transfers will help the Commission bypass some of Parliament's privacy concerns.

In order to form a legal basis for transferring the data, one possible option the Commission could explore is changing the purpose of the agreement so that it would fall under the European Privacy Directive. This way the agreement could be authorized under Article 25 of the European Privacy Directive. If the purpose was no longer the prevention of terrorism,

108. *E.C. Plans Framework to Give PNR Data to U.S.*, BUSINESS TRAVEL NEWS, June 19, 2006 at ¶ 1, available at http://www.btmag.com/businesstravelnews/headlines/article_display.jsp?vnu_content_id=1002690427.

it would not be considered an issue of national security. One possibility would be to change the objective of the agreement to protect the EUs travel industry. Without an agreement that is acceptable to both sides, the travel industry could be severely affected. The agreement could be considered a necessary measure to maintain and improve the European air carriers' success.

The EU and United States found acceptable solutions in the past, such as the Safe Harbor program, which allows U.S. companies to do business with EU Member States in a way that satisfies the EUs privacy laws and the needs of companies within the United States.¹⁰⁹ A similar program could be implemented in which the CBP could agree to abide by the EUs laws in a manner that is satisfactory to the United States regulations and the privacy concerns of the EU. This would require additional negotiations between the Commission and United States.

The Commission could also choose to forego an agreement altogether and instead create a new Council Directive that would change the policy for air travel to or through the United States. Rather than creating an agreement that would require approval through the European Privacy Directive, a new directive could be established, mandating certain rules and regulations for air carriers flying to U.S. airports. Council would have the authority to create a directive, with approval from Parliament, under Articles 94 and 95 of the EC Treaty. This may be difficult because a unanimous Council vote is required, but remains a possibility.

VI. CONCLUSION

The ECJs decision dated May 30, 2006 will have a potentially significant impact on the European travel industry beginning October of this year. The Council and Commission must pull their resources together to avoid an interruption of air carrier travel to the United States from the EUs Member States. They have had a relatively short amount of time to negotiate new terms that are acceptable to both the United States and EU. While a new approach would be the best option, drafting an entire new agreement in such a short amount of time is difficult, considering the initial agreement took about two years to finalize. It will be interesting to see what kind of solution they will find and if Parliament will be satisfied with the Commission's new recommendation.

The Council and Commission must take the following factors into consideration when drafting the new agreement: the stated objective of the agreement or directive; the EUs privacy laws regarding the transfer of personal data; U.S. regulations on flights into the United States; the

109. See U.S. Department of Commerce Homepage, Safe Harbor, <http://www.export.gov/safeharbor/index.html> (last visited Aug. 3, 2006).

appropriate legal basis for creating a new directive or international agreement; and the procedures to be followed in accordance with the EC Treaty. All of these issues will be carefully examined by Parliament once the new solution is proposed to ensure compliance with the EUs laws.

Another important goal is to reach a solution that is satisfactory to the Member States, which will be bound by the new agreement or directive. This should not pose a problem since the Member States will need this new solution in order to continue flights from air carriers in their respective countries into the United States. Hopefully the European Community will draft an agreement or directive that will successfully prevent an interruption of travel into the United States from EU destinations and will result in a lasting solution to the conflict between the U.S. travel regulations and EUs laws.

VII. UPDATE

There have been new developments since this article was written. The European Union (EU) and United States did not meet the September 30, 2006 deadline, but were able to reach an interim agreement on October 6, 2006.¹¹⁰ The interim agreement provided that the Department of Homeland Security (DHS) would access the passenger name record data from air carriers' reservations systems, but only until a new system was developed that would allow the air carriers to transmit the information to DHS.¹¹¹ The interim agreement remained in place until July 31, 2007.¹¹² The EU and United States then entered into a new agreement, which was approved by the EU General Affairs and External Relations Council.¹¹³ This new agreement was signed on August 4, 2007 and included an exchange of letters between the United States and EU with promises from the United States to the EU regarding how they will process and handle the PNR data.¹¹⁴ The agreement calls for a push system to be in place by January 1,

110. *See generally* Agreement Between the European Community and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, U.S.-Eur., Oct. 27, 2006, 2006 O.J. (L 298) 29, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_298/l_29820061027en00290031.pdf (last visited Aug. 28, 2007).

111. *Id.* at 30.

112. *Id.*

113. *See generally* Agreement Between the European Community and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), U.S.-Eur., Aug. 4, 2007, 2007 O.J. (L 204) 18, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf (last visited Aug. 28, 2007).

114. *Id.*

2008¹¹⁵ and requires less information than the prior agreement.¹¹⁶ It is expected that this agreement should resolve all of the disputes between the EU and United States regarding the transmission of PNR data, at least for the next seven years while the agreement is in place.¹¹⁷

115. *Id.* at 19.

116. *Id.* at 21–22.

117. *Id.* at 19.