(FLY) ANYWHERE BUT HERE: APPROACHING EU-US DIALOGUE CONCERNING PNR IN THE ERA OF LISBON

Douglas Louks*

I. INTRODUCTION

On September 11, 2001, nineteen terrorists boarded four planes in Newark, Boston, and Washington D.C. all headed to the west coast of the United States.[1] Shortly after takeoff, the terrorists onboard the planes subdued, by use of force, the flight attendants and pilots, thereby commandeering control of the aircraft.[2] On each plane was one terrorist trained to fly commercial aircraft.[3] Once in control, these terrorist-pilots took their aim for an attack at the heart of the American financial, government, and defense centers. Three of the aircraft hit their marks, successfully crashing, full of fuel, into World Trade Center 1 and 2 (The Twin Towers) in New York City and the Pentagon in Washington D.C. while the fourth, presumably aimed at the Capitol Building or the White House in Washington D.C., crashed in a field in Pennsylvania.[4] This single, intricate, and irreprehensible plan of terror carried out by Al Qaeda minions forever changed the landscape of our nation and the world. Specifically, the interplay between the right to privacy and national security, including the War on Terror, came into the crosshairs of the American government which took action thereby foisting US ideas of security upon those with whom it interacted.

A. US Action

Just a few months after the 9/11 attacks, the United States Congress passed the Aviation and Transportation Security Act (ATSA).[5] The ATSA

---

* J.D. Candidate, Indiana University – Robert H. McKinney School of Law (2013), M.B.A. University of Wisconsin-Whitewater (2010), B.A. Purdue University (2006). This author would like to acknowledge Dr. Frank Emmert for his invaluable guidance and advisement which greatly aided the production of this note. Lastly, and most importantly, the author thanks his wife Lisa for her unwavering love, support, tolerance, and dedication, without which none of this would have been possible.

1. *See* THE 9/11 COMMISSION REPORT EXECUTIVE SUMMARY 2 (2001) [hereinafter 9/11 COMMISSION REPORT], *available at* http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf.

2. *Id.* at 2

3. *Id.*

4. *Id.* at 1-2.

5. Irfan Tukdi, Note, *Transatlantic Turbulence: The Passenger Name Record Conflict*, 45 HOUS. L. REV. 587, 588 (2008). .

contains a specific provision which requires all foreign and domestic airline carriers flying into or over the United States to provide the Commissioner of Customs with a bevy of passenger and crew information.[6] The ATSA further requires all commercial aircraft arriving in the United States from a foreign country to electronically transmit a passenger arrival manifest, concerning the information of all aboard, to the Customs and Border Protection systems.[7] The information in this manifest includes credit card information, name, date of birth, gender, and more.[8] For those airlines which fail to comply and transmit this information before or soon after departure, a heavy fine, at the very least, could be imposed and, at most, their right to land the plane on American soil could be denied.[9]

B. The European Union's Response

With the great risk of planes being forbidden access to land on US runways, the air carriers of the European Union (EU) were placed in a rather precarious situation. They could either abide by Directive 95/46, the central legislation governing the protection of data and privacy in the EU, or grant the US authorities access to the personal data of their transatlantic passengers.[10] The airlines, in the face of monetary loss, chose the latter. The parties (the EU and the United States) entered into negotiations after enactment of the ATSA to develop conditions for an arrangement dealing with the transmission of the required passenger information.[11] Eventually, the EU and the United States agreed to terms on the Passenger Name Record (PNR) Agreement signed in 2004 by the Commission of the EU and by Tom Ridge, on behalf of the US Department of Homeland Security

6. 49 U.S.C. § 44909(c) (Supp. IV 2004) ("Not later than 60 days after the date of enactment of the Aviation and Transportation Security Act, each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to the Commissioner of Customs by electronic transmission a passenger and crew manifest containing the information specified [by the Act].").

7. *Id.*

8. Megan Roos, Note, *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union over Passenger Name Information*, 14 TRANSNAT'L L. & CONTEMP. PROBS. 1137, 1139-40 (2005).

9. Tukdi, *supra* note 5, at 588-89. *See also* Matthew R. VanWasshnova, Note, *Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned From the Existing System of Financial Information Exchange*, 39 CASE W. RES. J. INT'L L. 827, 833 (2007-2008) ("Airlines that did not comply with ATSA could be subject to fines or a revocation of landing rights.").

10. *See generally* Tukdi, *supra* note 5, at 589-90.

11. *See generally* Joint Statement, European Commission/US Customs Talks on PNR Transmission (Feb. 17-18, 2003), *available at* http://ec.europa.eu/transport/air/doc/security_2003_02_17_prn_joint_declaration.pdf.

(DHS).[12]

The European Parliament objected to the PNR Agreement at nearly every point of the process.[13] Just a few months after the PNR Agreement took effect, the European Parliament filed suit against the Council and Commission of the EU challenging the legality of the PNR claiming it was a direct violation of the privacy and data protection rights guaranteed by Directive 95/46/EC.[14] In 2006, the European Court of Justice (ECJ) annulled the PNR of 2004 for lack of legal basis[15] which, in short, was more of a procedural ruling than a substantive one.[16] As such, the Commission, after being given leeway for an interim agreement,[17] simply changed the agreement to give them the appropriate legal basis while leaving everything pertaining to the actual data transference the same and signed this 'new' PNR agreement with the United States in 2007 to run through 2013.[18] The legality of the 2007 PNR Agreement was never been challenged in the ECJ because, being based outside of the first pillar, the European Parliament did not retain the requisite authority to do so.[19]

C. Current Situation

Even though the 2007 PNR Agreement was not slated to end until 2014 at the latest,[20] the EU and the United States were forced to re-enter negotiations on the terms of a new PNR agreement to replace the 2007 PNR

---

12. *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, Bureau of Customs and Border Protection, 2004 O.J. (L 183) 84-85 [hereinafter 2004 PNR Agreement].

13. *See* Tukdi, *supra* note 5, at 590.

14. Joined Cases C-317/04 & C-318/04, Parliament v. Council, Comm'n, 2006 E.C.R. I-4798, 1-4826 [hereinafter 2006 ECJ Decision].

15. *Id.* at I-4831. Prior to the current status of the EU Treaties, the EU had a pillar structure with 3 pillars representing different competences granted to different institutions of the European Communities (Union). The EP only had authority to challenge legislation that was enacted in the first pillar. The Commission then changed the legal basis from the first pillar, which would have fallen under the 95/46 Directive, to another pillar. For a more in-depth explanation of the former pillar structure, see http://news.bbc.co.uk/2/hi/in_depth/europe/euro-glossary/1216944.stm.

16. 2006 ECJ Decision, *supra* note 14, at I-4828-29.

17. *Id.* at I-4832. *See generally* Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, 2006 O.J (L 298) 29 [hereinafter Interim Agreement].

18. *See* Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), 2007 O.J. (L 204) 18 [hereinafter 2007 PNR Agreement].

19. *See infra* III.D.

20. S. Res. 174, 112th Cong. (2011) (enacted).

Agreement due to a failure to ratify it prior to the entry into force of the Treaty of Lisbon in 2009.[21] The Treaty of Lisbon granted all international agreements, including the 2007 PNR Agreement, a new legal basis requiring European Parliament's approval in addition to a Council Decision in order to take effect.[22] In their new role, while retaining their disdain for the previous EU-US PNR agreements, the European Parliament refused to approve the 2007 PNR Agreement which forced new negotiations.[23]

Due to the general sentiment in the EU towards openness in government and politics, the draft of the new PNR Agreement was made available for scrutiny prior to its eventual approval.[24] However, there was also a confidential report from the legal advisors of the Commission touting the negotiated PNR Agreement as illegal[25] which was leaked to the media.[26] An agreement was eventually reached between the EU and the United States which was ratified by the European Parliament and Council[27] and entered into force on July 1, 2012.[28] What this report brought to light was that the terms of the proposal, which comprised the terms of the 2012 Agreement, are still at odds with EU law regarding data privacy and protection, perhaps even more so than the 2007 PNR Agreement which was

---

21. Hans Graux, *Belgian Passenger Name Record Approval Act Survives Legal Challenge on Procedural Grounds*, TIME.LEX (Apr. 12, 2011), http://www.timelex.eu/en/blog/detail/belgian-passenger-name-record-approval-act-survives-legal-challenge-on-procedural-grounds.

22. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 188 N, Dec. 17, 2007, 2007 O.J. (C 306) 97 [hereinafter Treaty of Lisbon]. *See also* Consolidated Version of the Treaty on the Functioning of the European Union art. 218, Mar. 30, 2010, 2010 O.J. (C 83) 144-45 [hereinafter TFEU] (In the amended version, this article appears as Article 218).

23. Sally McNamara, *European Parliament Should Back EU-US Passenger Name Record Agreement*, THE HERITAGE FOUNDATION (Sept. 6, 2011), http://www.heritage.org/research/reports/2011/09/eu-us-passenger-name-records-and-the-european-parliament.

24. Draft Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Record Data to the United States Department of Homeland Security, May 20, 2011, EU Doc. No. 10453/11 [hereinafter 2011 Proposal], *available at* http://www.statewatch.org/news/2011/may/eu-usa-pnr-agreement-20-5-11-fin.pdf.

25. Note from the European Commission Legal Service to Mr. Stefano Manservisi, Director General, DG Home (May 18, 2011) [hereinafter Legal Service Report] *available at* http://www.statewatch.org/news/2011/jun/eu-usa-pnr-com-ls-opinion-11.pdf.

26. Alan Travis, *Air Passenger Data Plans in US-EU Agreement are Illegal, say Lawyers*, THE GUARDIAN (Jun. 20, 2011, 14:45 EDT), http://www.guardian.co.uk/world/2011/jun/20/air-passenger-data-plans-illegal.

27. Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, Dec. 8, 2011, EU Doc. No. 17434/11 [hereinafter 2012 Agreement].

28. Information Concerning the Date of Entry into Force of the Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, July 4, 2012, 2012 O.J. (L 174) 1.

previously applied.[29] One major reason for the strong conflict is the entry into force of the Treaty of Lisbon which took place in December of 2009.[30] An important attribute of the Treaty of Lisbon is that it gives the Charter of Fundamental Rights of the European Union (CFR) legally binding effect.[31] The legal service for the EU Commission stated in its confidential memo that the terms of the draft agreement violate some of the fundamental rights which the CFR confers upon EU citizens.[32] The terms in the finalized 2012 Agreement are identical to the 2011 Proposed Agreement and thus the Commission Legal Service's memo is still relevant. In addition to this bout with the reality that the new agreement may infringe on fundamental rights, the European Parliament, which has been persistently critical of PNR agreement's with the United States since the inception of negotiations in 2003, now has more authority in these decisions than prior to the Lisbon Treaty.[33]

D. The Scope of This Note

Part II of this Note discusses the history and general sentiment of privacy and data protection in both the EU and the United States. This discussion includes a brief historical analysis of the events leading up to the 9/11 attacks, laws which relate to data protection and privacy in general, and laws developed which are pertinent to the debate concerning PNR. The purpose of this historical segment is to support an analysis of the laws and PNR agreements as well as to aid in making proposals for the resolution of the current PNR dilemma.

Part III provides an in-depth analysis of EU and US law which affect the PNR dialogue. In addition, this part examines both the 2007 PNR Agreement and the 2012 Agreement in light of the changes made to primary EU law by the Treaty of Lisbon, including the binding authority of the CFR.

In Part IV, building off of the analysis of Parts II and III, three possible options are discussed for the future of EU-US PNR agreements whereby one is recommended as the best solution to the current problem.

29. *See* Travis, *supra* note 26.
30. *See* Graux, *supra* note 21.
31. Treaty of Lisbon art. 6.
32. Legal Service Report, *supra* note 25.
33. Treaty of Lisbon art. 188 N.

PART II. THE HISTORY OF PRIVACY AND DATA PROTECTION IN THE EU AND US.

A. US – History and General Sentiment toward Privacy and Data Protection

1. 9/11 and the Reactionary Legislation

"September 11, 2001, was a day of unprecedented shock and suffering in the history of the United States."[34] On that fateful day, nineteen hijackers boarded planes on the eastern seaboard headed for the west coast under the orders and orchestration of Usama Bin Laden and his terrorist group, al-Qaeda.[35] The death toll was astonishing, surpassing that of December 1941, when the Japanese bombed Pearl Harbor.[36] In all, nearly 3,000 people lost their lives that day.[37] Shortly thereafter, in November 2001, then President George W. Bush ordered an extensive investigation into the events of, and those leading up to, the attacks: The 9/11 Commission.[38]

Perhaps most astonishingly, the events that transpired September 11 were seemingly quite preventable. As the 9/11 Commission stated, "The nation was unprepared."[39] The attackers and the plot by a group of extremists exploited major gaps in security and information sharing within the United States. The hijackers were 19 for 19 getting through the security checkpoints at the various airports.[40] The US authorities had ample information and intelligence, but no one could connect the dots. "[N]o analytic work foresaw the lightning that could connect the thundercloud to the ground."[41] As the 9/11 Commission found in their research of the events:

> Operational failures...included[:] not watchlisting future hijackers Hazmi and Mihdhar, not trailing them after they traveled to Bangkok, and not informing the FBI about one future hijacker's U.S. Visa or his companion's travel to the United States;... not discovering false statements on visa applications; not recognizing passports manipulated in a

34. 9/11 COMMISSION REPORT, *supra* note 1, at 1.
35. *Id.* at 3.
36. *Id.* at 2.
37. *Id.* at 2-3 ("More than 2,600 people died at the World Trade Center; 125 died at the Pentagon; 256 died on the four planes.").
38. *See generally id.*
39. *Id.* at 1.
40. *Id.* at 7.
41. *Id.*

> fraudulent manner; not expanding no-fly lists to include names from terrorist watchlists; not searching airline passengers identified by the computer-based CAPPS screening system[.][42]

In addition, part of this attack was comprised of "a cell of expatriate Muslim extremists who had clustered together in Hamburg, Germany."[43] The so-called 'Hamburg Cell' made extensive use of air travel dating from a few years prior to 9/11 up to the time they boarded their final flights.[44]

In order to remedy the vulnerabilities in the system of aviation security and data collection and transfer, the 9/11 Commission made several suggestions including "expanding no-fly lists, searching passengers identities by the CAPPS screening system, deploying federal air marshals domestically, hardening cockpit doors, [and] alerting air crews to a different kind of hijacking possibility than they had been trained to expect."[45] The plan behind these suggestions was to "[t]arget terrorist travel...Develop strategies for neglected parts of our transportation security system...[P]revent arguments about a new computerized profiling system from delaying vital improvements in the "no-fly" and "automatic selectee" lists...Determine...guidelines that integrate safeguards for privacy and other essential liberties."[46]

The legislative response to the inquiry regarding how to amend these vulnerabilities in order to protect the United States and its citizens was the enactment of the Aviation and Transportation Security Act of 2001(ATSA).[47] The ATSA requires that airlines submit the PNR for all flights into, out of, or within the United States to the United States Customs and Border Patrol (USCBP).[48] Essentially, this means pretty much every flight that enters US airspace. PNR data includes such things as "passengers' names, credit card information, and even meal preferences."[49] Failure of the airline to comply with the US requirement could result in rather large fines of up to $5000 per passenger.[50] At most, the United States can refuse to allow the airplane to land on US soil at all and may even revoke the landing privileges of that airline.[51]

---

42. *Id.* at 8-9.
43. *Id.* at 5.
44. *Id.*
45. *Id.* at 10.
46. *Id.* at 19.
47. Aviation and Transportation Security Act of 2001, Pub. L. 107-71, §101, 115 Stat. 597, 597-604.
48. *Id.* § 115.
49. Tukdi, *supra* note 5, at 588.
50. 19 C.F.R. § 122.161 (2007).
51. 19 C.F.R. § 122.14(d)(5) (2007).

2. General US Sentiment Toward Privacy

The United States generally has a quite different view and sentiment of privacy than that of other countries, especially those countries which are Member States in the EU. There is the Fourth Amendment of the US Constitution which protects a person from an unwarranted search and seizure.[52] However, as this amendment was written in 1791 and is not incredibly precise, attempting to apply it to the modern day computer-age notion of data and privacy protection can be quite problematic at times. There is also the judicial right to privacy, most notably upheld in the Supreme Court cases Griswold v. Connecticut[53] and Roe v. Wade.[54] But, there is no real 'right' of privacy in the United States, per se, which is to say there is no fundamental right to privacy. This framework, as will be discussed, is quite different than that of the EU.

The United States employs the sectoral approach to privacy. This basically means that the United States protects privacy on a point-by-point basis, picking and choosing when and where to employ privacy protection.[55] For the most part, Americans are generally more willing to barter privacy freedoms for security than are Europeans which is in large part due to the sectoral approach of American privacy laws. As one commentator puts it, "The United States' sectoral approach is more reactive in nature . . . .[T]he United States allows the market to decide how much privacy is needed, and the public generally has limited statutory rights."[56] The words of David Heyman, Assistant Secretary for Policy at the DHS, support this sentiment:

> Passengers have a right to privacy and protections of their civil liberties and personal information, but also have a right to know that their government is doing everything it can to ensure their safety and security when they board an airplane. It is necessary, therefore, to ensure the continued use of proven and effective security measures. PNR is a proven asset in the fight against terrorism and other

52. U.S. CONST. amend. IV.

53. Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (combining the First, Third, Fourth, Fifth, and Ninth Amendments to create a new constitutional right, the right to privacy in marital relations).

54. Roe v. Wade, 410 U.S. 113, 152 (1973) (Though the US Constitution does not "explicitly mention any right to privacy...the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.").

55. VanWasshnova, *supra* note 9, at 830-32.

56. Arthur Rizer, *Dog Fight: Did the International Battle Over Airline Passenger Name Records Enable the Christmas-Day Bomber?*, 60 CATH. U. L. REV. 77, 81-82 (2010).

transnational crimes.[57]

The United States really has only one piece of legislation that has a broad, blanketing effect with regard to data privacy and that is the Privacy Act of 1974.[58] This "single, wide-ranging data privacy law in the United States--the Privacy Act of 1974--restricts the use of personal data held by federal agencies. The Act requires federal agencies to apply 'fair information practices' to all agency policies regarding personal data sharing."[59] Even in this 'broad' legislation, there are some equally broad exceptions which punch holes in its effect. "The Privacy Act, however, does permit the disclosure of personal data for 'routine use' and subsequent interpretations of that provision have significantly weakened the effectiveness of the law."[60] The 'routine use' exception, as time passes and it is construed more broadly, will continue to erode any of the encompassing effect it would have had. As a consequence, the exception may possibly become the rule.

Not even a week after the 9/11 attacks, the willingness of the United States to trade-off privacy and data rights in exchange for national security became quite apparent. Congress, at this time, proposed legislation "to expand the surveillance and investigative powers of federal law enforcement agencies."[61] The result was enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act").[62] The PATRIOT Act greatly increased the ability of federal agencies to gather and transfer massive amounts of personal data.[63] Further, this legislation also restricted both public oversight and the public's power to contest the data collection.[64] Ambiguity in the terms used in the PATRIOT Act expanded the variety of data that could be procured.[65] For example, "[i]n June 2003, U.S. Attorney General John Ashcroft testified in front of the House Judiciary Committee

57. David Heyman, Assistant Sec'y, Office of Policy, Testimony before the House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence: Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel (Oct. 5, 2011) [hereinafter Heyman Testimony], *available at* http://www.dhs.gov/ynews/testimony/20111005-heyman-info-sharing-privacy-travelers.shtm.

58. 5 U.S.C. § 552(a) (1974).

59. D. Richard Rasmussen, *Is International Travel Per Se Suspicion of Terrorism? The Dispute Between the United States and European Union over Passenger Name Record Data Transfers*, 26 WIS. INT'L L.J. 551, 564 (2008).

60. *Id.* at 565.

61. *Id.* at 568.

62. *Id.*

63. *Id.*

64. *Id.*

65. *See id.*

that the term 'tangible things' subject to FBI seizure under the USA PATRIOT Act included personal data such as purchase records, computer files, educational records, library records, and genetic information."[66]

Congress did attempt to rein in the expansive collection of personal data to protect individual privacy through the creation of privacy offices.[67] "The new offices, however, have done little of consequence and the push by the executive branch for information sharing has continued with only limited oversight from Congress and the Supreme Court."[68] Given the recent signing of a four-year extension to the PATRIOT Act,[69] it appears that this readiness to barter privacy for security is not in recession nor is it likely to be any time in the near future.

3. EU – History and General Sentiment toward Privacy and Data Protection

European countries and their citizens tend to have a much different view of privacy than do most Americans. "European standards on the protection of the right to privacy are significantly different from American standards, as demonstrated by the fact that the creation of the PNR system was met with much greater resistance in the EU than in the US."[70] From the inception of negotiations between the EU and the United States, the members of European Parliament, as well as many citizens of the EU, were adamantly against the idea.[71] On the contrary, there was very little of this sentiment reciprocated across the pond.

A possible reason for this distinction between the EU and the United States with regard to privacy and data protection are the "historical roots."[72] Nazis were renowned for their use of data collection in order to track and account for Jews which nearly allowed for the mass extermination of an entire race of people in Europe.[73] After the fall of the Third Reich, citizens of Europe were then confronted by the autocratic Communist regimes which, as with the Nazis, relied heavily on data collection in order to squelch the voice of any threatening opposition.[74] Though Western

---

66. *Id.*

67. *Id.* at 570.

68. *Id.*

69. Jim Abrams, *Patriot Act Extension Signed by Obama*, THE HUFFINGTON POST (May 27, 2011 1:55 AM), http://www.huffingtonpost.com/2011/05/27/patriot-act-extension-signed-obama-autopen_n_867851.html.

70. Alenka Kuhelj, *The Twilight Zone of Privacy for Passengers on International Flights Between the EU & USA*, 16 U.C. DAVIS J. INT'L L. & POL'Y 383, 408 (2010).

71. Michael Kerr, *USA: Uncle Sam is watching you*, THE TELEGRAPH (July 19, 2003 12:01 AM), http://www.telegraph.co.uk/travel/727918/USA-Uncle-Sam-is-watching-you.html.

72. Kuhelj, *supra* note 70, at 408-09.

73. *Id.* at 409.

74. *Id.*

Europeans were not directly subjected to these same regimes as the citizens of Eastern Europe, this procurement of data and the way in which the data was used was certainly feared by them.[75] Given the recent history, it is fairly easy to empathize with Europe's contra-US perspective concerning personal data as the United States has never been subjected to a similarly fascist dictatorship. As one commentator has advanced: "The atrocities that followed the abuse of personal data in Europe, and the fact that the US has not had similar negative experiences with data protection, makes the different conduct and attitude to the collection, storage, and use of PNR understandable."[76]

Pursuant to the European position on the protection of data and privacy, it is reasonable to understand why, in the EU, privacy and data protection are applied through a very broad, comprehensive, and robust approach. First, both data protection and privacy are covered by encompassing legislation such as that of Directive 95/46.[77] They were also given the status as fundamental rights[78] after the entry into force of the Treaty of Lisbon.[79] Well before the Treaty of Lisbon, several countries in Europe drafted and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) thereby placing data protection and privacy in the context of human rights throughout Europe.[80] Second, the privacy guaranteed by these laws applies whenever and to or by whomever it is processed, transmitted, or stored.[81] It is not a case-by-case basis as a norm like that in the United States, but rather instilled in almost all contexts.[82]

Another distinction between the EU and United States in this regard is that, in the United States, "privacy interests on a scale [are] counterbalanced by free speech rights," while in the EU, they "analogize privacy rights with

---

75. *Id.*

76. *Id.*

77. *See e.g.*, Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive 95/46].

78. Charter of Fundamental Rights of the European Union, art. 7-8, 2000 O.J. (C 364) 1 [hereinafter CFR]. *See also* Kuhelj, *supra* note 70, at 409.

79. Treaty of Lisbon art. 6; *see also* Consolidated Version of the Treaty on European Union art. 6, Mar. 30, 2010, 2010 O.J. (C 83) 19 [hereinafter TEU] (granting the CFR legally binding effect equal to that of the Treaties).

80. *See Convention for the Protection of Human Rights and Fundamental Freedoms: Status,* COUNCIL OF EUROPE (Feb. 5, 2013), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=05/02/2013&CL=ENG (demonstrating the current countries that have ratified the Convention); *see also Convention for the Protection of Human Rights and Fundamental Freedom* (Nov. 4, 1950), *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf [hereinafter ECHR].

81. *See, e.g.*, Directive 95/46, *supra* note 77.

82. Tukdi, *supra* note 5, at 591.

intellectual property rights."[83] The viewpoint here is that "[i]f government is going to let corporations keep competitors from exploiting brand-names and trademarks, the law certainly should allow a citizen to keep others from trafficking in his credit history, sex life and other personal information."[84] As a result, the laws and legislation of the EU and Member States treat an individual's data as something in line with proprietary information.

It was with the variant sentiments concerning data and privacy in combination with the reactionary post-9/11 US legislation, the EU and the United States entered into negotiations for a PNR scheme that would bring the air carriers flying from the EU to the United States in compliance with the ATSA. The Commission and the United States finally agreed to terms on an agreement in 2004[85] which was later annulled by the ECJ based on the challenge of the European Parliament that it was in direct violation of Directive 95/46.[86] In the end, the ECJ annulled based on a technicality, an incorrect legal basis.[87] The Commission, in response, simply moved the basis from the first to the third pillar which resulted in the European Parliament losing their voice and ability for legal challenge.[88] During the time that the 2007 PNR Agreement was implemented, the primary law in the EU drastically changed with the entry into force of the Treaty of Lisbon.[89] European Parliament's regained voice as a consequence of the Treaty of Lisbon caused a new round of negotiations for an EU-US PNR agreement.[90] The next section analyzes the former and current PNR agreements in light of these treaty changes and Directive 95/46.

III. ANALYSIS OF APPLICABLE EUROPEAN UNION LAW

A. Directive 95/46

Directive 95/46, passed in 1995, is the legislative embodiment of the European sentiment toward the protection of privacy and personal data.[91] The Data Protection Directive also further differentiated the approach of the EU to that of the United States with regard to the protection of data and data

83. Tanya L. Forsheit, et al., *Privacy, Data Security and Outsourcing*, 946 PLI/PAT 11, 18 (2008).

84. *Id.*

85. *See e.g.* 2004 PNR Agreement, *supra* note 12.

86. Tukdi, *supra* note 5, at 590; *see also* ECJ Decision, *supra* note 14, at I-4831.

87. ECJ Decision, *supra* note 14, at I-4831.

88. Elspeth Guild & Evelien Brouwer, *The Political Life of Data: The ECJ Decision on the PNR Agreement Between the EU and the US*, CENTRE FOR EUROPEAN POLICY STUDIES POLICY BRIEF, July 2006, No. 109 at 3.

89. Rizer, *supra* note 56, at 98; *see also* Treaty of Lisbon.

90. Rizer, *supra* note 56, at 99; *see also* 2011 Proposed Agreement, *supra* note 23.

91. Rizer, *supra* note 56, at 83.

privacy.[92] For the EU, finding the US approach of the non-comprehensive protection of privacy to be inadequate, the only effective way to protect data was through a blanket approach.[93] The preamble of Directive 95/46 illustrates this perspective of the EU sentiment by stating:

> [D]ata processing systems are designed to serve man...they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy[.] . . . The fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive[.][94]

As is the case with all directives, the purpose of Directive 95/46 was to standardize pertinent legislation across all of the Member States.[95] To accomplish this, the Directive "proposes strict requirements on the processing of personal data."[96] The Directive states:

> [A]ny processing of personal data must be lawful and fair to the individuals concerned[.]...[I]n particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed[.]...[S]uch purposes must be explicit and legitimate and must be determined at the time of collection of the data[.][97]

The Directive further provides that "in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary...for the performance of a task carried out in the public interest[.]"[98] The latter portion of this provision potentially allows for a lot of discretion. So long as the personal data is necessary for the greater public interest, the directive seems to allow its process. However, to curtail the use of such a gap, the directive states that "data...capable... of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent[.]...[D]erogations from this prohibition must be explicitly provided for in respect of specific needs[.]"[99] To help determine what this actually means, Article 7 states that other than

92. VanWasshnova, *supra* note 9, at 832.
93. *Id.*
94. Directive 95/46, *supra* note 77, pmbl.
95. Rasmussen, *supra* note 59, at 559.
96. *Id.*
97. Directive 95/46, *supra* note 77, pmbl.
98. *Id.* pmbl., Recital 30.
99. *Id.* Recital 33.

by personal consent of the subject, personal data may be processed in "compliance with a legal obligation."[100] Lastly, the Member States are prohibited from processing of the so called 'sensitive data' which includes "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[101]

Directive 95/46 does permit the transfer to personal data to third countries, but only if that nation "ensures an adequate level of protection."[102] It also mandates that "the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited[.]"[103] The Directive further requires that "the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations[.]"[104] In the event the Commission finds that any country provides inadequate data protection, the Member States are strictly prohibited from transferring any personal data to that country until the Commission, through negotiation, can fix the issues.[105] Interestingly, the United States was found to be one such country which did not provide adequate protection of European data which required the approval of certain safe harbor provisions for commercial transactions.[106]

A major concern for the EU regarding the Directive was oversight to ensure that the directive was being applied correctly and that no circumvention of the law took place which is both evidenced and alleviated by Articles 28 and 29.[107] Article 28 requires that every Member State establish its own independent enforcement body.[108] Article 29 establishes a Working Party on the protection of individuals with regard to the processing of personal data.[109] The Article 29 Working Party is comprised of a representative from each Member State, a representative for the Community, and one from the Commission.[110] This is an independently working group that has an advisory capacity on the nature of data protection.[111] The Working Party may give an opinion on any act or legislation affected by the Directive whether or not they are expressly asked

100. *Id.* art. 7.
101. *Id.* art. 8.1.
102. *Id.* art. 25.
103. *Id.* pmbl. Recital 57.
104. *Id.* pmbl. Recital 56.
105. VanWasshnova, *supra* note 9, at 830.
106. *Id.* at 832.
107. Directive 95/46, *supra* note 77, arts. 28-29.
108. *Id.* art. 28.
109. *Id.* art. 29.
110. *Id.*
111. *Id.*

to do so.[112] The Working Party can only give an opinion to the Commission which is non-binding in nature.[113] However, the Commission must address any opinion given by the Working Party and the reasoning for diverging from that opinion.[114] In addition, both the Working Party's opinions and the Commission's reasoning for diverging from or acting in accordance with such opinions must be made public.[115] Therefore, though the opinions are not binding, making them available to the public in conjunction with the requirement that the Commission answer for its action in public, can act as a check on the Commission's power by exerting political pressure on the Commission.

Even though Directive 95/46 was meant to be a very broad and comprehensive data protection law, there is one very large gap left by the scope of the Directive.

> This Directive shall not apply to the processing of personal data...in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security...and the activities of the State in areas of criminal law[.][116]

This provision grants a wide exemption. Basically, anything that falls outside of Community law, meaning the first pillar (in the former pillar structure), was exempt. With the fall of the pillar structure brought on by the entry into force of the Treaty of Lisbon,[117] the processing of data pursuant to or for the necessity of public security, defense, security, and criminal law remains part of this exemption.[118] However, for other reasons, discussed later, this exemption may not matter in the context of PNR Agreements between the EU and the United States.

B. 2004 PNR and 2006 Annulment

When the United States enacted the ATSA, the laws of two powers on each side of the Atlantic Ocean were placed into immediate conflict with

---

112. *Id.* art. 30.
113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.*, art. 3.2.
117. *Treaty of Lisbon: Introduction*, EUROPA, July 14, 2010, http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0033_en.htm (last visited May 18, 2013).
118. Directive 95-46, *supra* note 75, pmbl., Recital 13.

one another. Meanwhile, European airlines were stuck in the middle between a figurative 'rock and a hard place' because no matter which path they chose, they would have been subject to a fine.[119] "The airlines that complied with the ATSA by transferring passenger data violated EU privacy laws; however, refusal to transmit the data to U.S. authorities meant facing fines and the possible revocation of landing rights."[120] The airline companies had to transmit or allow the US authorities access to the data either before or shortly after takeoff and the fine for refusal to comply could reach as much as $5,000 per passenger.[121] From a purely financial perspective, the European airlines were left without any real choice in this matter seeing that compliance with EU law would have led to massive losses to the airlines through the stiff monetary penalty and potential loss of landing privileges.[122] The United States did, however, grant a waiver to the European airlines until the EU and United States could work out a permanent deal, but this waiver to penalize noncompliant European airlines ended in March of 2003 and many of these European airlines granted the United States access to their PNR data.[123] On account of this, the EU and United States immediately entered into negotiations for a firm agreement.[124] The parties finally agreed to a deal on May 17, 2004.[125]

However, a major point of contention for the countries was the Commission's decision on the adequacy of US protection of EU citizens' data. The Commission's decision was based almost exclusively on a letter from the USCBP to the Commission detailing what they would undertake in the gathering and processing of PNR data.[126] In June 2003, the Article 29 Working Party gave their opinion which "expressed doubts regarding the level of data protection" guaranteed by the US authorities.[127] The Article 29 Working Party, named so as their function and creation is based on Article 29 of Directive 95/46, was very apprehensive of the 2004 PNR Agreement for a few reasons:

> [T]he European Data Protection Working Party . . . repeatedly raised its doubts on the proportionality of transfer of PNR data and on the level of protection as guaranteed in the undertakings of the US . . . (CBP). Other concerns dealt with the fact that the transfer of data was

119. Guild & Brouwer, *supra* note 88, at 1-2.
120. Rizer, *supra* note 56, at 87.
121. Guild & Brouwer, *supra* note 86, at 1.
122. Tukdi, *supra* note 5, at 589.
123. 2006 ECJ Decision, *supra* note 14, at I-4822.
124. *Id.*
125. *See generally* 2004 PNR Agreement, *supra* note 12.
126. Commission Decision 2004/535, 2004 O.J. (L 235) 12 (EC).
127. 2006 ECJ Decision, *supra* note 14, at I-4823.

based on a 'pull' instead of 'push' system . . . .[128]

The Article 29 Working Party believed that the sheer amount of data that was requested was unnecessary to the function to which it would serve.[129] They were also quite concerned about the USCBP having access to the European airlines' reservation systems and taking the data as opposed to the airlines transmitting the data to the USCBP.[130]

Despite this, the Commission, pursuant to the former Article 300 of the Treaty of the European Community, submitted the agreement with the United States to the European Parliament for a consultation based on their own decision that the USCBP "provid[ed] an adequate level of protection."[131] The European Parliament delayed in giving their opinion on the adequacy of the Agreement despite the Council requesting an urgent opinion.[132] Two weeks after the Commission's submission, the European Parliament adopted a resolution detailing its apprehension to the proposed agreement and asked the Commission to draft a new agreement.[133] As the European Parliament had refused to give their opinion on the adequacy of the Commission's draft decision, the Commission passed its decision on adequacy which the Council adopted on May 17, 2004, as the 2004 PNR Agreement.[134] The European Parliament then challenged this agreement on the basis of the involvement of both the Council and the Commission for their respective roles.[135]

The ECJ annulled the 2004 PNR Agreement on the grounds that it lacked appropriate legal basis.[136] The 2004 PNR Agreement was based in the first pillar transport policy, but the ECJ held that since the agreement was for security and combating terrorism, it should fall under the public security framework, a third pillar provision.[137] Article 3(2) of the Directive states that it "shall not apply to the processing of personal data...in the

128. Guild & Brouwer, *supra* note 88, at 2.

129. Article 29 Data Protection Working Party, *Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*, 11221/04/EN, WP 95 (June 22, 2004), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp95_en.pdf.

130. *Id.*

131. 2004 PNR Agreement, *supra* note 12, at 84.

132. 2006 ECJ Decision, *supra* note 14, at I-4823.

133. *Id.*

134. *Id.* at I-4823-24.

135. *Id.* at I-4826.

136. *Id.* at I-4831.

137. Guild & Brouwer, *supra* note 88, at 3.

course of an activity which falls outside the scope of Community law," meaning data processing that occurs outside the first pillar.[138] As such, the ECJ held that the Directive did not apply to the 2004 PNR Agreement or the adequacy decision, but that the Commission did not have the appropriate competence in the first pillar.[139]

In essence, this was a purely procedural ruling and, unfortunately, appears to lend little to no substantive quality that could be applied to either the 2007 PNR Agreement or the 2011 Proposal, and thereby the 2012 EU-US PNR Agreement (2012 PNR Agreement), to determine their legality. "The ECJ did not take an explicit position on whether the PNR Agreement disproportionately encroached on the rights of EU citizens, but instead took an easier course and annulled the Council Decision and Commission Decision on formal grounds."[140] However, the ECJ annulment may not totally lack meaning. For instance, the ECJ began its opinion by citing to Article 8 of the ECHR which states the right to individual privacy and also "the circumstances in which a state may intervene with the right."[141] This was the first known instance of the ECJ doing anything of this nature by referring to an international human rights agreement as opposed to EU law, especially given that at that time the EU was not a party to the ECHR.[142] There are a few possible theories as to why the ECJ would reference the ECHR. At the time of this ruling by the ECJ, the Treaty establishing a Constitution for Europe (EU Constitution) was in the ratification period.[143] The EU Constitution would have given the EU legal personality[144] and thus allowed the EU to accede to the ECHR.[145] Therefore, it is possible that the ECJ was trying to be politically influential to push the ratification of the EU Constitution and express its view of accession to the ECHR. In addition, it is a quite reasonable assumption that the ECJ was predicting that in future PNR disputes, the ECHR's personal privacy provisions would play an important role.

C. The Treaty of Lisbon

Quite possibly the most important and influential change in EU law took place on December 1, 2009 when the Treaty of Lisbon entered into

---

138. Directive 95/46, *supra* note 77, art. 3(2).

139. Guild & Brouwer, *supra* note 88, at 3.

140. Kuhelj, *supra* note 70, at 400.

141. Guild & Brouwer, *supra* note 88, at 2-3.

142. *Id.* at 3.

143. Carlos Closa, *The Constitution Ratification*, THE EUROPEAN UNION CONSTITUTION, http://www.proyectos.cchs.csic.es/euroconstitution/Treaties/Treaty_Const_Rat.htm (last visited May 18, 2013).

144. Treaty establishing a Constitution for Europe art. I-7, Dec. 16, 2004, 2004 O.J. (C 310) 13.

145. *Id.* art. I-9.

force.[146] The adoption of the Treaty of Lisbon made four extremely significant amendments to the TEU and TFEU that affect the PNR debate. First, it adopted the Charter of Fundamental Rights of the European Union (CFR) as primary law equal to that of the Treaties.[147] Second, through the Treaty of Lisbon, the EU acceded to the ECHR thus bringing the institutions and all Member States within the jurisdiction of the European Court of Human Rights (ECtHR).[148] Third, the Treaty of Lisbon granted far more legislative and political power to the European Parliament by collapsing the three pillars of the EU, thereby eradicating the former pillar structure.[149] Lastly, the European Parliament was further empowered by the Treaty of Lisbon by the change in the legislative process. Prior to the amendments, the Treaty Establishing the European Communities (EC Treaty) Article 251 called for the consultation method of passing legislation.[150] The Treaty of Lisbon changed this to a co-decision method requiring joint decision-making between the Council and the European Parliament.[151] All of these changes to the Treaties will undoubtedly have an immeasurable impact on the future of PNR negotiations and agreements between the EU and the United States

The Commission exclusively negotiated the PNR agreements of 2004, 2006, and 2007; negotiation being a sole function of the Commission.[152] Prior to the Treaty of Lisbon, the European Parliament only had a right to consultation regarding the drafting of such agreements.[153] However, this right of consultation was only available if the action fell within the competence of the European Community, meaning the first pillar.[154] For the 2004 PNR Agreement, the Commission and Council merely granted a token nod to the European Parliament by consulting them on the drafts of the agreements.[155] For the 2006 Interim Agreement and the 2007 PNR Agreement, there was no longer a necessity to involve the European Parliament since each was moved under the third pillar, a Union

146. Graux, *supra* note 21.

147. Treaty of Lisbon art. 6(1).

148. *Id.* arts. 6(2)-6(3).

149. *Structure of the Treaties Governing the EU*, CITIZENS INFORMATION BOARD (Feb. 8, 2010), http://www.citizensinformation.ie/en/government_in_ireland/european_government/eu_law/lisbon_treaty/structure_of_the_treaties_governing_the_eu.html.

150. Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, Oct. 2, 1997, 1997 O.J. (C 340) 280; Treaty Establishing the European Communities art. 251 [hereinafter EC Treaty] (as in effect until Dec. 1, 2009) (now TFEU art. 294).

151. Treaty of Lisbon art. 251 (amending EC Treaty art. 251, which is now TFEU art. 294).

152. TEU art. 17.

153. EC Treaty art. 251.

154. VanWasshnova, *supra* note 9, at 838.

155. Guild & Brouwer, *supra* note 88, at 3.

competence, effectively circumventing the European Parliament in the process.[156]

Under the amendments of the Treaty of Lisbon, the circumstances surrounding the 2006 and 2007 Agreements would be completely untenable. The amendments made to the Treaties collapsed the pillars into one, the first pillar, which thereby brings all Commission and Council action within the same competence as the European Parliament.[157] In addition, the Treaty of Lisbon also eliminated the consultation procedure of legislative enactment, which resulted in very limited involvement by the European Parliament, and replaced it with the co-decision procedure.[158] Subsequent to the Treaty's enactment, the European Parliament became, and currently is, a resounding voice in the negotiations and the future of the EU-US PNR relationship. Currently,

> Except where agreements relate exclusively to the common foreign and security policy, the Council shall adopt the decision concluding the agreement after obtaining the consent of the European Parliament in the following cases . . . agreements covering fields to which either the ordinary legislative procedure applies, or the special legislative procedure where consent by the European Parliament is required.[159]

In short, the European Parliament, together with the Council, will decide on all actions which do not involve the common defense and security policy, which is more akin to military type action or prevention and does not include PNR, which falls under the Home Affairs Commission.[160]

Another significant amendment to the Treaties made by the Treaty of Lisbon was adopting the CFR originally meant to be part of the EU Constitution, and further giving the CFR the status of primary EU law. "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."[161] The purpose of the CFR is "to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those

156. *Id.*; *see also* VanWasshnova, *supra* note 9, at 838.

157. Treaty of Lisbon arts. 24-25(b).

158. *Id.* art. 9 C.

159. *Id.* art. 188 N.

160. *See generally* EUROPEAN EXTERNAL ACTION SERVICE, http://www.consilium.europa.eu/eeas/security-defence (last visited May 18, 2013). *See also* Legal Service Report, *supra* note 25 (the report is addressed to the Directorate General of the Home Affairs).

161. Treaty of Lisbon art. 1(8).

rights more visible in a Charter."[162] The fundamental rights which are contained within the Charter, as such rights, cannot be infringed upon or violated; they are guaranteed rights, unless their limitation is "necessary and genuinely meet[s] objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[163] In addition, the limitation of a right must be proportional to the objective.[164]

Data protection for an individual, after the Treaty of Lisbon, attained the status of a fundamental right pursuant to the CFR. Article 8 of the CFR states:

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[165]

Even if Directive 95/46, for any reason, does not apply to PNR agreements or is somehow rendered less effective through gaps in the legislation or otherwise, the CFR will still be applicable and protect personal data. Thus, the PNR debate will hinge on whether the data is processed fairly, proportionately, and legitimately by law for the general interest.

Yet another important change made by the Treaty of Lisbon was EU accession to the ECHR.[166] By the EU acceding to the ECHR, yet another layer and set of rights will take effect with regard to the EU itself. In 1950, the countries comprising the Council of Europe[167] met in Rome to draft, and eventually sign, the ECHR.[168] "[T]his declaration aims at securing the universal and effective recognition and observance of the Rights therein declared...[with the purpose of] maintenance and further realization of human rights and fundamental freedoms."[169] Those countries which signed and thereby acceded to the ECHR took on the obligation to secure the freedoms and rights of all of the citizens within their jurisdiction.[170] This convention also created a judicial body known as the European Court of

162. CFR, *supra* note 78, pmbl.
163. *Id.* art. 52(1).
164. *Id.*
165. *Id.* art. 8.
166. Treaty of Lisbon art. 1(8).
167. This is not to be confused with the European Council, which is an EU institution; the Council of Europe has no affiliation with the EU.
168. ECHR, *supra* note 80, pmbl.
169. *Id.*
170. *Id.* art. 1.

Human Rights (ECtHR). [171]

All Member States of the EU were already party to the ECHR prior to the Treaty of Lisbon and therefore the citizens of those Member States could challenge the actions of their own country on the basis of human rights violations in the ECtHR .[172] After the Treaty of Lisbon, the citizens of the EU can challenge the actions of the EU directly, even when that action is to compel Member State action, as a violation of their individual human or fundamental rights.[173] Although the Treaty of Lisbon mandates accession to the ECHR,[174] actual accession by the EU to the ECHR has yet to occur.[175] As a consequence, a citizen can still challenge an EU act, but only to the extent that it is carried out in the national legislature; they cannot directly challenge any EU act in the ECtHR.[176]

Given the current status of the EU's official accession to the ECHR, in order for a citizen to challenge any PNR agreement in the ECtHR, there must be national law in place. This has created a rather difficult situation for the people of the EU because the 2007 PNR Agreement was not ratified prior to the entry into force of the Treaty of Lisbon.[177] With the entry into force of the Treaty of Lisbon, and therefore the subsequent greater legislative powers of the European Parliament, the 2007 Agreement was never ratified by the Parliament.[178] As such, the 2007 Agreement was only provisionally applied pursuant to a 2007 Commission Decision "which rules that the Agreement should be provisionally applied pending its entry into force."[179]

Another issue with the provisional application in the context of the ECHR is that in order to open the gates to the ECtHR, one must exhaust all other judicial remedies: "The Court may only deal with the matter after all domestic remedies have been exhausted[.]"[180] For citizens of the EU, this requires the exhaustion of the national court system as well as in the ECJ. The ultimate result is that the fundamental and human rights of the citizens of the EU were placed in limbo in the context of an ECtHR. However, it does appear that accession of the EU is to come in the near future.[181] Regardless of when this accession does in fact occur, there is no doubt that

171. *Id.* art. 19.

172. *EU Accession to the European Convention on Human Rights*, COUNCIL OF EUROPE, http://www.coe.int/lportal/web/coe-portal/what-we-do/human-rights/eu-accession-to-the-convention (last visited May 18, 2013) [hereinafter COUNCIL OF EUROPE].

173. *Id.*

174. Treaty of Lisbon art. 1(8)(2); *see also* TEU art. 6(2).

175. COUNCIL OF EUROPE, *supra* note 172.

176. *Id.*

177. Rizer, *supra* note 56, at 99.

178. McNamara, *supra* note 23.

179. Graux, *supra* note 21.

180. ECHR, *supra* note 80, art. 35.

181. COUNCIL OF EUROPE, *supra* note 172.

the mandate for accession in the Treaty of Lisbon will have a dramatic effect on the state of PNR.

All of the amendments made to the Treaties by the Treaty of Lisbon will have incredible bearing and weigh very heavily on the state of current and all future PNR negotiations and agreements. As the European Data Protection Supervisor stated in a 2010 opinion, "It is essential that any agreement with third countries takes into account the new data protection requirements as they are being developed in the post-Lisbon institutional framework."[182]

D. 2007 PNR

After the 2004 PNR Agreement was annulled, the ECJ allowed for the Commission to negotiate an interim agreement in 2006 to satisfy the United States and to prevent yet another major dilemma for the European airlines.[183] Just days prior to the expiration of the 2006 Interim Agreement, the United States and EU agreed to terms on a new PNR deal which was signed in Brussels on July 23, 2007 and in Washington on July 26, 2007.[184] The Commission, when drafting the 2007 PNR Agreement, did make some other minor changes from the 2004 Agreement, most notably answering the demand to change from the 'pull' to the 'push' method.[185] But, for the most part, it basically just changed the legal basis from the first pillar of the European Communities competence to the third pillar invoking Articles 26 and 38 of the TEU.[186]

There were a few important issues regarding the change from the first pillar to the third. "For one, in the third pillar the Parliament has even less voice than in the first pillar, so the result would be that the Parliament is effectively cut out of the picture."[187] In the third pillar, the European Parliament did not have the competence to challenge the Commission or the Council as they had in the ECJ in 2006. Second, by this move, Directive 95/46 became wholly inapplicable to the PNR Agreement since the scope of

182. Opinion of the European Data Protection Supervisor on the Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries of 30 Dec. 2010, 2010 O.J. (C 357) 11 [hereinafter EDPS Opinion 2010].

183. *See generally* Interim Agreement, *supra* note 17.

184. 2007 PNR Agreement, *supra* note 18.

185. *Id.* The 2004 Agreement allowed the US to 'pull' data, which means to access the airlines' computer reservation systems (CRS) and thereby gain access to and review the data. *Id.* The 'push' method is simply the opposite where the airlines send the DHS the PNR data. *Id.*

186. *Id.* After the Treaty of Lisbon, former Article 24 became Article 37 in the TEU and former Article 38 has since been repealed (*see* Treaty of Lisbon Annex *Table of Equivalents* 2007 (C306) 202-229).

187. Guild and Brouwer, *supra* note 86, at 3.

the Directive does not include "the processing of personal data in the course of an activity which falls outside the scope of Community law, such as...processing operations concerning public security, defence, States security . . . and the activities of the State in areas of criminal law[.]"[188] The third pillar concerned "matters of policing and criminal law" and thus was not within the grasp of the Directive.[189] Third, the ECJ could also have been effectively excluded from ruling on PNR after the move to the third pillar.[190] ECJ "jurisdiction over third-pillar matters depends on whether each member state has made a declaration permitting its national courts . . . to refer questions to the ECJ on third pillar issues."[191] However, after the Treaty of Lisbon entered into force, these factors became much less relevant, and possibly irrelevant altogether.

Given that the 2007 Agreement was not ratified before the Treaty of Lisbon entered into force, it was only provisionally applied and thus it needed to be ratified by the European Parliament in order to be fully effective, which is to say "formally enforced."[192] This consent was never given by the European Parliament and they declined to ratify the 2007 Agreement as recently as May 2010.[193] Politically, the PNR agreements between the EU and the United States have never been popular with the European Parliament.[194] However, there may also be a sound legal basis for the European Parliament's adamant opposition. In order to fully understand the 2012 Agreement, one must delve into the applicable laws and apply them to the 2007 Agreement in order to fully understand the 2012 Agreement as well as to determine if this new agreement is an improvement and whether it fits within the EU legal framework.

With the Treaty of Lisbon entering into force and thereby collapsing the former pillar structure of EU law, the third pillar basis of the 2007 PNR Agreement was no longer sufficient to circumvent application of Directive 95/46 because it was outside the Directive's scope, at least as it pertains to the pillar competences.[195] The pertinent portions of Directive 95/46 which need to be analyzed in order to determine whether the 2007 PNR Agreement meets the strict requirements of the Directive are Articles 6, 8, 12, 13, and 25.

Article 6 sets out the basic principles dealing with data processing. With regard to PNR, the pertinent sections state:

188. Directive 95/46, *supra* note 77, art. 3(2).
189. Guild & Brouwer, *supra* note 88, at 3.
190. *Id.* at 4.
191. *Id.* at 3.
192. McNamara, *supra* note 23.
193. *Id.*
194. Rizer, *supra* note 56, at 99.
195. Guild & Brouwer, *supra* note 88, at 4.

> [T]hat personal data must be . . . adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed . . . accurate . . . [and] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[196]

The first part of this is a matter of proportionality, which is a key component of the EU legal system. The information collected and processed must be proportional to the purpose for its collection, which is for security and to prevent terrorism and other types of organized crime.[197] This has been a major point of contention for privacy advocates who are opposed to the agreements as well as the European Parliament and the Article 29 Working Party.[198] Both the European Parliament and the Article 29 Working Party have found that the amount of data available in the 2007 PNR was excessive in relation to purpose for its transfer.[199]

The data that was collected and included in PNR was very extensive. In all, there were nineteen types of PNR data collected and required for transfer to US authorities.[200] This number, though a reduction from the amount of elements collected, processed, and transferred in the 2004 Agreement, "is a mere subterfuge as the [2007] Agreement groups all but one of the thirty-four elements into one of the nineteen new data sets."[201] Despite this reduction, the 2007 "Agreement retains broad categories such as 'general remarks' and 'all historical changes to the PNR.'"[202] Therefore, it can be inferred that the reduction in categories was by no means an actual reduction in the PNR data that is collected and transferred. The European Parliament, specifically referring to the array of data and the relation to

196. Directive 95/46, *supra* note 77, art. 6.

197. 2007 PNR Agreement, *supra* note 18, at 18.

198. Guild & Brouwer, *supra* note 88, at 2; *See also* Tukdi, *supra* note 5, at 610.

199. European Parliament Resolution on SWIFT, the PNR Agreement and the Transatlantic Dialogue on These Issues, 2007 O.J. (C 287 E) 349, 351 [hereinafter European Parliament Resolution 2007]; *See also* Article 29 Data Protection Working Party, *Opinion 7/2010 on European Commission's Communication on the Global Approach to Transfers of Passenger Name Record (PNR) data to third countries*, 622/10/EN, WP 178, at 3 (Nov. 12, 2010) [hereinafter Article 29 Working Party 2010 Opinion], *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178_en.pdf.

200. Letter from Michael Chertoff, U.S. Secretary of Homeland Security, to Luis Amado, President of the Council of the European Union, 2007 O.J. (L 204) 21-22 [hereinafter DHS Letter]. *See also* 2007 PNR Agreement, *supra* note 18, at 19 (the DHS letter is more or less part of the 2007 Agreement incorporated in the first recital of the agreement as a basis for reliance on the part of the European Union and follows sequentially in the Official Journal.)

201. VanWasshnova, *supra* note 9, at 839.

202. Rasmussen, *supra* note 59, at 586-587.

their legitimate use, stated:

> [I]t would seem that in practice, for law enforcement and security purposes, Advance Passenger Information System (APIS) data are more than sufficient; these data are already collected in Europe in accordance with Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems (2), and may therefore be exchanged with the US under a comparable regime; behaviour data in the PNR seem to be of limited use, as they cannot be identified if not linked to APIS; the justification for the general transfer of PNR data is therefore not satisfactory[.][203]

The Article 29 Working Party further stated that, though "personal data can be valuable under certain circumstances," it still may not be enough to guarantee air travel security and that less intrusive measures should also be employed with regard to innocent passengers.[204] Given the excessive amount of data that were collected through the 2007 Agreement, it is possible that the volume did not fit within the framework of Article 6 of the Directive.

Article 8 provides that certain personal data, called sensitive data, cannot be processed except with the consent of the subject.[205] Such data includes "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[206] The 2007 Agreement provided that the United States would automatically delete any such sensitive data that is included in any of the PNR data transferred to the DHS.[207] However, the United States still retained the ability to access that data "in exceptional case[s]"[208] or if it may threaten US interests.[209] Additionally, "the deletion of sensitive data applies only in principle, and in prac[t]ice [sic] the US itself w[ould] decide what constitutes grounds for deletion."[210] This exception for the collection of sensitive data, even if only in extremely exceptional cases, was what the European Data Protection Supervisor (EDPS) stated was utterly deplorable.[211] "He consider[ed] that the

203. European Parliament Resolution 2007, *supra* note 199, at 351.
204. Article 29 Working Party 2010 Opinion, *supra* note 199, at 3.
205. Directive 95/46, *supra* note 77, art. 8.
206. *Id.*
207. DHS Letter, *supra* note 200, at 22.
208. *Id.*
209. Kuhelj, *supra* note 70, at 405.
210. *Id.* at 404-405.
211. EDPS Opinion 2010, *supra* note 182, at 10.

conditions of the exception are too broad and do not bring any guarantees[.]"[212]

In addition to the other articles, Article 12 directly correlated to the 2007 PNR Agreement. This article provides that the subject must have a right of access to the data collected concerning them and also that they have the right to rectify any error in that data which hearkens back to the requirement for the accuracy of data being processed in Article 8 of the Directive.[213] The obvious purpose for this provision was so that any and all data subjects could ensure and also be assured that the data being transferred which is identifiable to them is indeed correct.

The 2007 PNR Agreement did grant some access, stating, "Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR."[214] This information, when requested, was to be "disclosed to the individual in accordance with the Privacy Act and the US Freedom of Information Act (FOIA)."[215]

Even though the agreement provided for this right of access, US compliance with this provision may be lacking. In February of 2010, the DHS promulgated a final rule exempting the Automated Targeting System (ATS), the system where PNR data is stored, from the requirement for disclosure of the Privacy Act, even though this is a "flagrant violation of the DHS 'undertakings' and the DHS-EU 'agreement'."[216] On account of this, "non-US persons are not being afforded the greater access rights provided by the Privacy Act."[217] Even when explicitly requested on the basis of the Privacy Act, the information, if divulged at all, has only been done so in accordance with the FOIA, meaning only data that is required to be released by the FOIA is released.[218] According to a study by the Identity Project, none of the requests for PNR data have been performed by the DHS in accordance with the Privacy Act, only in accordance with the FOIA.[219] Additionally, "All DHS responses . . . have been incomplete."[220] Without US compliance, the 2007 Agreement appeared to clearly be in violation of Article 13 of the Directive.

---

212. *Id.*

213. Directive 95/46, *supra* note 77, art. 12.

214. DHS Letter, *supra* note 200, at 23.

215. *Id.*

216. The Identity Project, *DHS "Update" Still Misstates Compliance with EU Agreement on PNR Data*, PAPERS, PLEASE! BLOG ARCHIVE (Apr. 18, 2010 1:31 PM), http://www.papersplease.org/wp/2010/04/18/dhs-update-still-misstates-compliance-with-eu-agreement-on-pnr-data/.

217. *Id.*

218. *Id.*

219. *Id.*

220. *Id.*

The noncompliance of the United States with regard to the right of access brings to light an imperative notion. Most of the 2007 Agreement, that is the promises or "assurances", were given by the United States in the form of a letter from Michael Chertoff, US Secretary of the DHS, to Luis Amado, President of the Council (DHS Letter).[221] Many of the specific provisions of the 2007 Agreement are contained in the DHS Letter, not the actual body of the Agreement itself.[222] However, the DHS Letter, which holds so many specifications, was not legally binding in nature.[223] As one scholar stated, "[I]t is significant that the processing, collection, use, and storage of personal data are not regulated by a bilateral agreement (or on international law), but only on the transient 'assurances' in the US Letter, which may change at any time."[224] The 2007 Agreement was anchored only "[o]n the basis of the assurances" which was rather problematic for the EU, or should have been seen as such.[225] This is further supported by a 2007 Resolution of the European Parliament which stated that the assurances "must become an integral part of the agreement and must be legally binding."[226]

In addition to the aforementioned articles, Article 25 was a central point of contention as it allowed the transfer of data from the Member States to a third country, provided that the third country in question provided "an adequate level of protection."[227] The criteria used in determining the adequacy of data protection of a third country included, most importantly, but not limited to, "the nature of the data, the purpose and duration of the proposed processing operation or operations . . . the rules of law, both general and sectoral, in force in the third country in question . . . and security measures which are complied with in that country."[228] A couple of issues arose in the context of this Article when discussing the duration of data retention as well as the rule of law in the United States.

The DHS Letter stated that the United States had the authority to hold the PNR data of an individual for up to fifteen years; seven years in active status and eight years in dormant status.[229] Some scholars have been quite critical of the length of this retention period as it is nearly five times the length of retention provided for in the 2004 Agreement.[230] It is possible that

221. *See generally* DHS Letter, *supra* note 200.
222. *Id.*
223. *Id.*
224. Kuhelj, *supra* note 70, at 404.
225. 2007 PNR Agreement, *supra* note 18, at 19.
226. European Parliament Resolution 2007, *supra* note 199, at 352.
227. Directive 95/46, *supra* note 77, art. 25.
228. *Id.*
229. DHS Letter, *supra* note 200, at 23.
230. VanWasshnova, *supra* note 9, at 839 ("[T]he Revised Agreement[] extends the retention period from three and one-half years to fifteen years, with the possibility of it being extended further.").

such an extensive retention period could be in violation of Article 6 of the Directive which states that data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which" the data were collected.[231] In contrast, the EU draft agreement with Australia only has a retention period of five and one-half years (three years active and two and one-half years dormant statuses) and a recent proposal for an EU PNR Directive only contained a retention period of a little over five years (thirty days active and five years dormant statuses).[232] Given that the 2007 Agreement was still almost three times the length as another EU PNR agreement and the proposed directive, it does appear it was unnecessary for the purpose served.

The 2007 Agreement applied the US Privacy Act protections to the data subjects involved in the PNR transfers.[233] However, "the Agreement does not afford full Privacy Act protections to the PNR data collected by DHS, other than the disclosure of data to individuals; thus, DHS will be permitted to share the data with other federal, state, and local law enforcement agencies."[234] In a sense, this means that the United States could do what they please with the data once they had received it. Further degrading the adequacy of protection, "[t]he US Privacy Act only protects its own citizens against abuse and incorrect use of personal data[.]"[235] It seems apparent that if an EU citizen has no legal rights to recourse on the basis of US law then their data would not be adequately protected by the United States.

In light of this information, it does not seem likely that the 2007 Agreement was in line with the provisions of Directive 95/46 mainly in regard to the lack of adequate protection of data in the United States. However, Articles 3 and 13 granted wide exemptions for data processing and use when its collection was a matter of security or defense.[236] Therefore, even though the Treaty of Lisbon, by collapsing the pillar structure, may have brought all PNR agreements within the first pillar and thus subject to the Directive, this may not be enough to protect the data subjects.[237] Given that the ECJ in their 2006 Decision held that the 2004 Agreement was for public security, it is very possible that they would have ruled similarly with regard to the 2007 Agreement, which would have exempted it from subjectivity to the Directive.[238] However, it must be noted that the Article 29 Working Party adamantly holds their ground that any

231. Directive 95/46, *supra* note 77, art. 6(1)(e) (emphasis added).
232. Legal Service Report, *supra* note 25.
233. DHS Letter, *supra* note 200, at 23.
234. Rasmussen, *supra* note 59, at 587.
235. Kuhelj, *supra* note 70, at 413-414.
236. Directive 95/46, *supra* note 77, arts. 3 and 13.
237. Guild & Brouwer, *supra* note 88, at 4.
238. ECJ Decision, *supra* note 14, at I-4828.

and all PNR agreements must comply with Directive 95/46.[239]

Despite the possibility that the 2007 Agreement and future PNR agreements would fall outside the scope of Directive 95/46, after the Treaty of Lisbon these agreements must abide by rules for protection of fundamental rights established in the CFR and also be added to the TFEU.[240] As the European Commission Legal Service wrote in their letter to the Director General of the Home Affairs Commission:

> [A]n international agreement to be concluded by the Union must, like any other act of secondary law, [] comply with primary law, including fundamental rights...this requires in particular the respect of the right to the protection of personal data enshrined in Article 16 TFEU and Article 8 of the Charter of Fundamental Rights.[241]

In particular, "this means that any restriction of that fundamental right must be limited to what is necessary and proportional."[242]

The CFR is quite explicit in its protection of privacy and data. Article 7 grants, "Everyone has the right to respect for his or her private and family life, home and communications."[243] In addition, Article 8 provides for protection of personal data, that all "data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law."[244] Given their very nature as fundamental rights as well as their addition to Treaties pursuant to the Treaty of Lisbon granting the CFR the same legal effect of primary EU law, there is no doubt that these rights are directly applicable to PNR.[245]

As the Legal Service Report states, since the right to privacy and data protection are fundamental, any limitation of those rights must be proportional and necessary. Article 52 of the CFR specifically states:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to

239. Article 29 Working Party 2010 Opinion, *supra* note 199.
240. *See generally* CFR, *supra* note 78; *See also* TFEU art. 16.
241. Legal Service Report, *supra* note 25.
242. *Id.*
243. CFR, *supra* note 78, art. 7.
244. *Id.* art. 8.
245. TEU art. 6; *see also* Treaty of Lisbon art. 1.

protect the rights and freedoms of others.[246]

As has been demonstrated, security, which is the ECJ's stated purpose of PNR, could reasonably be considered to be 'general interest'.[247] In addition, as a stated purpose is public security and because terrorism can potentially be a serious threat to human lives, PNR could be said to be a 'need to protect the rights and freedoms of others', specifically the Article 2 right to life[248] and the Article 6 right to security of person.[249] Therefore, the 2007 Agreement, as well as future PNR agreements, may lawfully limit the fundamental rights to privacy and data protection if proportional and necessary. The Article 29 Working Party has already deemed the fight against terrorism and serious transnational crime necessary.[250] The Working Party "has always supported the fight against international terrorism and serious transnational crime" and "considers this fight necessary and legitimate."[251] This seems to be both a reasonable and agreeable view. Thus the issue of PNR agreements limiting fundamental rights of subjects comes down to proportionality.

The two main proportionality issues concerning the 2007 Agreement are retention period and the extent of the data. As stated previously, the retention period of the 2007 Agreement was an increase of nearly five times that of the 2004 Agreement, and three times that of the draft EU-Australian PNR Agreement.[252] The European Parliament refused to ratify this agreement partly on account of such a lengthy retention period.[253] Additionally, in the EU's own proposal for PNR for internal EU travel, the retention period was only five years.[254] The Article 29 Working Party stated that "retention periods should not be longer than necessary for the performance of the defined purpose."[255] Specifically, the Working Party finds that "[r]etention of data of non-suspected individuals raises the question of their necessity and might conflict with constitutional principles in some Member States."[256] It believes that unless the data of a passenger has triggered some sort of an investigation, it should be discarded immediately after analysis.[257] This short of a retention period may in actuality be too short and could possibly lower the working efficiency of

246. CFR, *supra* note 78, art. 52.
247. ECJ Decision, *supra* note 14, at I-4828.
248. CFR, *supra* note 78, art. 2.
249. *Id.* art. 6.
250. Article 29 Working Party 2010 Opinion, *supra* note 199, at 3.
251. *Id.*
252. *See* VanWasshnova, *supra* note 9, at 839.
253. Legal Service Report, *supra* note 25.
254. Travis, *supra* note 26.
255. Article 29 Working Party 2010 Opinion, *supra* note 199, at 6.
256. *Id.*
257. *Id.*

PNR systems in general. The Council Legal Service seems to believe that a retention period of two years is adequate for the purposes for which the data is held, but questioned the necessity of retention beyond that period.[258] Although there are varying opinions among different EU and independent bodies about what is the maximum retention period to remain proportional, as the Commission Legal Service stated, "[I]t appears highly doubtful that a period of 15 years can be regarded as proportional."[259]

The shear breadth and amount of data that was collected and processed pursuant to the 2007 Agreement also raises the issue of proportionality. There were nineteen categories of data that were or could have been collected by the DHS through the 2007 Agreement.[260] However, some of these categories were very broad such as "General Remarks" which allowed more data to be collected under the guise of just one category.[261] In addition, the 2007 Agreement still allowed the collection of the so-called 'sensitive data' which included data revealing religious beliefs, racial origin, ethnic origins, or political opinions.[262]

The issue is determining just how much information is needed to effectuate the purpose of PNR agreements to stop terrorism. The European Parliament has stated on at least two occasions that Advance Passenger Information (API) data is more than sufficient for the purpose served.[263] Also, the API data collection would be much less invasive on the personal privacy of data subjects than was the data collection in the 2007 PNR scheme.[264]

Lastly, it is the opinion of both the EDPS and the Article 29 Working Party that sensitive data should not be transferred to the DHS at all.[265] The EDPS specifically calls for a reduction of categories, including the broad categories like 'general remarks' as well as the 17th category named in the DHS Letter,[266] to eliminate the transmission of sensitive data.[267] The PNR data is needed to combat terrorism and serious international crime through

---

258. Legal Service Report, *supra* note 25.

259. *Id.*

260. DHS Letter, *supra* note 200, at 21-22.

261. Rasmussen, *supra* note 59, at 586-587.

262. *Id.* at 587.

263. European Parliament Resolution 2007, *supra* note 199, at 351; *see also* European Parliament Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) Agreements with the United States, Australia and Canada. 2011 O.J (C 81) E/73 [hereinafter European Parliament Resolution 2010].

264. European Parliament Resolution 2010, *supra* note 263, at E/73.

265. EDPS Opinion, *supra* note 180, at 10; Article 29 Working Party 2010 Opinion, *supra* note 199, at 6.

266. DHS Letter, *supra* note 200, at 22 ("General remarks including OSI [Optional Services Instruction], SSI [Special Services Instruction] and SSR [Special Service Request] information").

267. EDPS Opinion, *supra* note 180, at 10.

tracing of recent travel, credit card transactions, other financial information, and contact information.[268] However, sensitive data can be used in one way only which is to profile individual passengers.[269] The Article 29 Working Party does not believe that this is the most effective manner to alleviate the problem and certainly not the least invasive.[270] The Working Party specifically noted:

> The usefulness of large-scale profiling on the basis of passenger data must be questioned thoroughly, based on both scientific elements and recent studies. Up to now the Working Party has not seen any information confirming the usefulness of such profiling. On the contrary, recent studies tend to establish the counter-productive character of such screening, especially in relation to the fight against terrorism.[271]

Therefore, since the amount of PNR data that is transferred to the DHS may neither be the least invasive nor necessarily the most effective means of accomplishing the purpose, it seems the logical progression that the amount of PNR data transferred pursuant to the 2007 Agreement was not proportional.

E. 2011 PNR Proposal and 2012 Agreement

When the Treaty of Lisbon entered into effect, the 2007 Agreement had not yet been ratified, and therefore was not fully effective. Consequently, with their newly granted legislative powers, the European Parliament refused to ratify the 2007 Agreement and asked the DHS to enter negotiations for a new PNR agreement; the DHS obliged.[272] The negotiations between the European Commission and the DHS commenced in December of 2010 and an agreement on a text, the 2011 Proposal, was reached in May of 2011.[273] The resulting proposal was met with the similar rebuke as the 2004 and 2007 Agreements.[274] In contrast to the 2007 Agreement, the harshest admonition came from the Commission's own Legal Service which, in their opinion, seriously doubted the legality of the 2011 Proposal.[275] In particular, the Commission Legal Service had "grave

268. *Id.*
269. *Id.*
270. Article 29 Working Party 2010 Opinion, *supra* note 199, at 3.
271. *Id.* at 4.
272. Heyman Testimony, *supra* note 57.
273. *Id.*
274. *See generally* Travis, *supra* note 26.
275. Legal Services Report, *supra* note 25.

doubts as to [the proposal's] compatibility with the fundamental rights to data protection."[276] The 2011 Proposal was amended slightly culminating in the European Parliament's approval to become the 2012 EU-US PNR Agreement (2012 Agreement).[277] However, this did not include amendment of any of the provisions which the Commission Legal Service found problematic. Therefore, the service's report and the other criticisms of the 2011 Proposal are equally applicable to the 2012 Agreement.

The 2011 Proposal did address some of the issues that plagued the 2007 Agreement. As opposed to the EU basing almost an entire agreement with the United States on a legally non-binding letter of assurance, the integral provisions of the 2012 Agreement are rightfully set out in what would become a legally binding agreement.[278] For example, access for individuals, contained in the DHS Letter in the 2007 Agreement, is Article 11 in the 2011 Proposal.[279] In addition, the 2011 Proposal incorporates the 'push' method for data transfers, which was also previously covered by the DHS Letter.[280] These provisions, as with nearly all of the terms of the 2011 Proposal, were copied into the 2012 Agreement.[281]

Despite incorporating much of the DHS Letter into the legal framework of an agreement, the 2011 Proposal, and thereby 2012 Agreement, still fall below the legal standard required under EU law. For instance, although the 2012 Agreement does require the push method, there is still a wide exception that allows the DHS to acquire access to the carriers' systems "in order to respond to a specific, urgent, and serious threat[.]"[282] Additionally, the redress incorporated into Article 13, as with the 2007 Agreement, still "guarantees basically no judicial redress to data subjects, since all judicial redress is made subject to US law . . . [and] are administrative only and thus at the discretion of the DHS."[283] As with the 2007 Agreement, the oversight is not guaranteed to be independent which is required by Directive 95/46 Article 28.[284] Lastly, the 2012 Agreement also still allows the retention of sensitive data just as the 2007 Agreement.[285]

---

276. *Id.*

277. *See generally* 2012 Agreement, *supra* note 26.

278. *See generally* 2011 Proposal, *supra* note 24.

279. *Id.* art. 11.

280. *Id.* art. 15; *compare* DHS Letter, *supra* note 200, at 23 (Carriers had to comply with DHS requirements for 'push' method data transmission. For those who did not, the DHS still held the right to 'pull' data from their CRS directly until they could meet DHS requirements.)

281. 2012 Agreement, *supra* note 26, arts. 11 and 15.

282. 2012 Agreement, *supra* note 26, art. 15(5).

283. Legal Service Report, *supra* note 25; *compare* DHS Letter, *supra* note 200, at 23. (The one major difference is that the 2012 Agreement does not offer the US Privacy Act as protection to EU citizens as in the 2007 Agreement, only offering applicability of the FOIA).

284. Legal Service Report, *supra* note 25; *See also* Directive 95/46, *supra* note 77, art 28.

285. Travis, *supra* note 26. *See also* 2012 Agreement, *supra* note 26, art. 6.

The 2012 Agreement also makes some critical changes from the 2007 Agreement which may have caused it to violate the principles of proportionality and necessity even more than the 2007 Agreement. The 2011 Proposal attempted to expand the circumstances in which US authorities can process PNR data by replacing "transnational crime" with the much broader category of "[o]ther serious crimes, which shall mean extraditable offences as defined in Article 4 of the Agreement on Extradition between the United States and the European Union . . . that are transnational in nature."[286] Based on the extradition agreement, a serious crime is one which is punishable by more than one year.[287] With such a low maximum penalty as well as the transnational requirement being met by simply occurring in or affecting more than one nation,[288] which will inevitably "include a very large number of crimes which cannot be regarded as serious[,]" the proportionality of the agreement is put into question.[289] Another major sticking point of the 2012 Agreement provision is that applying the extradition agreement definition of serious crimes seems repugnant as those individuals are already suspected or convicted of the crime whereas PNR relates to "a priori innocent individuals."[290] The 2012 Agreement changes this provision for the proposal slightly to include only "[o]ther crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature."[291] This is still a low enough penalty to raise the same issues mentioned in the Legal Service Report bringing proportionality into question.

The Legal Service also finds that the third clause of Article 4, which would allow PNR to be used in identifying persons that would be further questioned and scrutinized at the borders of the United States also "raises serious questions of proportionality."[292] This is simply a means of extending the USCBP's capabilities to police immigration offenses, possibly very minor offenses, not a means of preventing terrorism or serious transnational crime.[293]

Within that same Article, yet another provision drew the ire of the Commission's Legal Service. Subsection 2 of Article 4 would allow the DHS to use and process PNR "if ordered by a court."[294] The Legal Service finds that this cannot possibly be a meaningful limitation as it would allow the use of PNR for any purpose provided that the user could persuade a US

286. 2011 Proposal, *supra* note 24, art. 4(b).
287. Legal Service Report, *supra* note 25.
288. 2011 Proposal, *supra* note 24, art. 4(b).
289. Legal Service Report, *supra* note 25.
290. *Id.*
291. 2012 Agreement, *supra* note 26, art. 4(1)(b).
292. Legal Service Report, *supra* note 25.
293. *Id.*
294. 2012 Agreement, *supra* note 26, art. 4(2).

judge to allow it.[295] This is a direct violation of Article 52 of the CFR which provides that a "limitation on the exercise of rights and freedoms . . . must be provided for by law[.]"[296] The Legal Service does not consider such a provision to meet the requirement of foreseeability which the ECJ has held is needed to uphold the principle of a measure's being provided for by law.[297]

One consistency between the 2012 Agreement and the 2007 Agreement is the retention period, which remains fifteen years.[298] However, the active period would be shortened to five years with a dormant period of ten years.[299] The proposal also provides that after six months, "PNR shall be depersonalized and masked[.]"[300] This is, quite simply, a hollow, empty promise of protection considering that the data could be 'demasked' by US authorities, albeit by "a limited number of specifically authorized officials."[301] The ending result is the same in that the data can be 'repersonalized' and utilized after it is masked if the United States desires it to be so. The Legal Service does not find such a reduction of the active status period to be enough to scotch the same proportionality concerns as the 2007 Agreement's retention period as it "represents almost no improvement compared to the [2007] EU-US agreement, which the Parliament refused to approve . . . ."[302] Despite a shorter active period and access being more restricted in the dormant period, the data can still be accessed by US authorities.[303] The bottom line is that fifteen years of retention is quite incongruous with the requirement of proportionality.

On account of these major conflicts with fundamental rights and data protection laws in the EU, the Legal Service came "to the conclusion that despite certain presentational improvements, the draft agreement does not constitute a sufficiently substantial improvement of the agreement currently applied on a provisional basis, the conclusion of which was refused on data protection grounds by the European Parliament."[304] As a matter of fact, the Legal Service viewed the 2011 Proposal as "a setback from the point of view of data protection."[305] For these reasons, there is no doubt, at least in the eyes of the Legal Service, that the 2011 Proposal violates the fundamental rights guaranteed to EU citizens by the CFR.[306] Given that the

295. Legal Service Report, *supra* note 25.
296. CFR, *supra* note 78, art. 52(1).
297. Legal Service Report, *supra* note 25.
298. 2012 Agreement, *supra* note 26, art. 8.
299. *Id.*
300. *Id.*
301. *Id.*
302. Legal Service Report, *supra* note 25.
303. *Id.*
304. *Id.*
305. *Id.*
306. *Id.*

2012 Agreement incorporated almost the exact same provisions of the 2011 Proposal the Commission's Legal Service found to violate the CFR, it stands to reason that the 2012 Agreement also likely violates the same fundamental rights of EU citizens.

IV. RECOMMENDATION

Given the information available, there appear to be three options that the EU can authorize, two of which have already been shown to be untenable with regard to fundamental rights. First, the EU, through the actions of the European Parliament as well as the other bodies, could annul the 2012 Agreement and then ratify the 2007 Agreement. The second option for the EU is to accept the new status quo held in the terms 2012 Agreement. Given that the 2007 Agreement has many of the same proportionality issues as the 2011 Proposal and thus the 2012 Agreement, which the Commission Legal Service deemed to violate fundamental rights, it seems logical that the 2007 Agreement also violates fundamental rights. As such, neither of these two options should be entertained by the EU. The final and recommended option is for the European Parliament to annul the 2012 Agreement and then for the European Commission to negotiate a new bilateral agreement with the United States. This new bilateral agreement should be consistent with the basic principles of EU law and the fundamental rights guaranteed by the CFR which was incorporated into primary EU law by the Treaty of Lisbon.

Instead of the broad, sweeping categories and breadth of PNR data that is transferred pursuant to the 2007 Agreement, the new agreement should use the much less invasive API data. In addition to being less invasive to privacy, the EU already has the appropriate legal framework in place concerning API data and it would be fairly easy to apply when sending it to the United States while, more than likely still providing an adequate amount of security to counter terrorism efforts and transnational crime.[307] As the European Parliament has already stated:

> [I]t would seem that in practice, for law enforcement and security purposes, Advance Passenger Information System (APIS) data are more than sufficient; these data are already collected in Europe in accordance with Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems, and may therefore be exchanged with the US under a comparable regime; behaviour data in the PNR seem to be of limited use, as

307. European Parliament Resolution 2007, *supra* note 199, at 351; *see also* Council Regulation (EEC) No. 2299/89 of 24 July 1989, 1989 O.J. (L 220) 1, 1.

> they cannot be identified if not linked to APIS; the justification for the general transfer of PNR data is therefore not satisfactory[.][308]

Regardless of whether the same API data is acceptable to the United States, any new agreement must eliminate any transfer of sensitive data to the United States, which would require the actual reduction of the categories of PNR data that is transferred. Further, on the basis of proportionality, any new agreement must also reduce the retention period. There is a wide variance in opinion as to what would be proportional, but it certainly must be less than fifteen years.[309] The best outcome would likely be a retention period of between five and six years which would bring the new agreement in line with the 2004 Agreement with the United States as well as the current draft agreement with Australia.[310]

Additionally, the new agreement must eliminate the criticisms of all other EU-US PNR agreements. The method of transfer should be exclusively push thereby eliminating the any ability of the United States to pull data from European airlines.[311]

It is also vitally important that EU citizens have knowledge of their data being transferred as well as access to their records in order to ensure their adequacy and accuracy.[312] "PNR data is unverified information, mostly provided by the passengers themselves or their tour operators or travel agencies and collected for business purposes, not law enforcement purposes. As there is no (easy) way to objectively verify these data, PNR data cannot be considered as exact information."[313] Based on this assessment, a subject's access to his or her records and data are necessary not just on account of this being a fundamental right,[314] but also for the effectiveness of data use. This is a point which US authorities ought to willingly agree being that any effective use of such data is contingent on the data being correct. If the people do not have access to the data or the ability to ramify any errors, the data becomes useless. US denial of concession to this point would be illogical.

The negotiation of a new EU-US PNR agreement based on these suggestions is not without problems. The biggest issues are the US Senate Resolution and the general administrative sentiment that any new agreement must not degrade the operational effectiveness of the 2007

308. European Parliament Resolution 2007, *supra* note 199, at 351.
309. Legal Service Report, *supra* note 25.
310. *Id.*
311. European Parliament Resolution 2007, *supra* note 199, at 352.
312. *Id.* at 351.
313. Article 29 Working Party 2010 Opinion, *supra* note 199, at 5.
314. CFR, *supra* note 78, art. 8.

Agreement.[315] It seems likely that any reduction to any of the terms stated in the 2007 Agreement would be considered by the United States to "degrade the usefulness of the PNR data for identifying terrorists and other dangerous criminals" and thereby compel DHS rejection of the agreement.[316]

The other major obstacle is that the entirety of all EU-US PNR relations has been dominated by the United States who has basically disregarded any notion of actual negotiation to conform to EU demands or to comply with EU laws.[317] Tony Bunyan of Statewatch, a group which keeps track of civil liberties across all of Europe, stated:

> Secret minutes of EU-US meetings since 2001 show that they have always been a one-way channel, with the US setting the agenda by making demands on the EU[.] When the EU does make rare requests, like on data protection, because US law only offers protection and redress to US citizens, they are bluntly told that the US is not going to change its data protection system – as they were at the EU-US JHA ministerial meeting in Washington on 8-9 December 2010.[318]

Yet another obstacle is that the United States entered into several bilateral agreements with different EU Member States which condition admission into the US Visa Waiver Program on those Member States providing the United States with PNR data.[319] Being that these PNR transfers are based on the 2007 Agreement's provisions, any degradation in the new agreement would seriously threaten these bilateral agreements.[320] The last and perhaps most problematic obstacle is that, both logistically and politically, it would be wildly unpopular and almost unthinkable that the EU would rescind an agreement which so recently entered into force and which was the culmination of nearly two years of negotiations.

However, the EU needs to stand their ground against the United States. The EU is really the "only legal check on the actions of the United States" being that they have the political clout and affluence necessary to control the United States in the international arena.[321]

What is more important than the EU asserting their position in the international political sphere, is the EU's need to limit the inevitable fallout

315. S. Res. 174, *supra* note 20; *see also* Heyman Testimony, *supra* note 57.
316. S. Res. 174, *supra* note 20.
317. Travis, *supra* note 26.
318. *Id.* (citing Bunyan during an interview for the article).
319. McNamara, *supra* note 23.
320. *Id.*
321. Rasmussen, *supra* note 59, at 589.

that will occur by enactment of an agreement that violates fundamental rights guaranteed by the CFR and the ECHR, to which all Member States have acceded.[322] "A solution within the EU . . . is highly desirabl[e] as the alternative is the potentially very damaging possibility of a judgment from the [ECtHR] striking down the EU-US agreement on human rights grounds."[323]

After the European Parliament and the Council approved the PNR agreement, the national legislations will now have to implement it into their own legal framework.[324] Once in the national legislation and thereby legally binding, the people of that nation will have access to their courts to challenge the agreement on the grounds that it violates their fundamental rights to privacy and data protection.[325] Because of the gravity and consequence, there are two possible outcomes, but the likely result is that the national court will refer the case to the ECJ for a preliminary ruling on the matter.[326] The ECJ could then either do what is easiest and annul any agreement that violated fundamental rights, such as the 2007 Agreement or the 2012 Agreement, or they could rule in favor of the Member State. Since all Member States have acceded to the ECHR, if, and only if, the ECJ hears the case and denies remedy for the individual can that person then apply to have the case heard by the ECtHR.[327] Once in the ECtHR, the case could prove very troublesome to the EU as "[i]t is to be doubted whether the transmission of the extensive list of personal data to US authorities and the uncertainty about the future use of this information will pass the test of the criteria which have been developed by the [ECtHR] on the basis of Article 8 ECHR."[328]

The ECtHR, which is wholly independent from the EU or its institutions, does not, nor has it ever, had any qualms with ruling Member State law as a violation of human rights, even when that means an inevitable imposition on US law as was seen in Soering v. United Kingdom.[329] The outcome of that case was that Soering's extradition from

322. CFR, *supra* note 78, arts. 7-8; ECHR, *supra* note 80, art. 8.

323. Guild & Brouwer, *supra* note 88, at 6.

324. TFEU art. 291.

325. *Id.* art. 291; *see generally* Graux, *supra* note 21.

326. TFEU art. 267. Even if the national court ruled in favor of the agreement, the matter could still be appealed up through national court systems to the ECJ. If the ECJ denied hearing the case, the sole option would be for the individual to apply to hear the case in the ECtHR.

327. ECHR, *supra* note 80, art. 35 ("The Court [ECtHR] may only deal with the matter after all domestic remedies have been exhausted").

328. Guild & Brouwer, *supra* note 88, at 4.

329. *See generally* Soering v United Kingdom, 11 Eur. Ct. H.R. (ser. A) (1989) (holding that Soering, a German national who was accused of committing capital murder in the State of Virginia and the fleeing to the United Kingdom, and who petitioned the ECtHR on the grounds that extradition to a place where he faced the death penalty violated his fundamental

the UK was deemed to violate his human rights on account of the State of Virginia seeking the death penalty, and the US State ultimately had to change its prosecution to seeking a life sentence in order to get extradition from the UK.[330] Since an individual has to exhaust all domestic remedies before he or she can seek remedy in the ECtHR,[331] it could mean that several years would have passed with the agreement in place before the ECtHR rules and if, as in the Soering case, they rule against the Member State, the EU would then be forced to negotiate an agreement that abided by fundamental rights immediately, not to mention the political fallout of the decision to annul an agreement as a violation of human rights. The risk of such a ruling is too high for the EU to gamble by not structuring a new agreement that does not comport with the fundamental rights of its people.

It is in consequence of all of this information that the only option for the EU regarding EU-US PNR agreements is to repeal the 2012 Agreement and then to negotiate a wholly new agreement which addresses all of the issues that have been brought to light, such as proper oversight of US data protection, judicial redress for EU citizens, and adherence to fundamental principles of EU law regarding necessity and proportionality. This has been further emphasized by a recent opinion of the European Data Protection Supervisor.[332] In this opinion, the EDPS stated that although the 2011 Proposal and thereby the 2012 Agreement "includes adequate safeguards on data security and oversight, none of the main concerns expressed...nor the conditions required by the European Parliament to provide its consent appear to have been met."[333] As such, neither the 2012 Agreement nor the 2007 Agreement fit within the legal framework of the EU as they either do not meet the requirements of Directive 95/46, the EU Founding Treaties as amended by the Treaty of Lisbon, or they come in conflict with certain fundamental rights guaranteed to EU citizens by the ECHR.

V. CONCLUSION

There is little argument to contest that the aftermath of events which transpired on September 11, 2001 have had a profound effect on law and privacy in the United States. With the proposed purpose of increased security, the immense transportation laws which were passed by the US Congress required other countries to negotiate bilateral agreements with the

---

human rights under Article 3 ECHR. The ECtHR ruled that UK extradition, despite their extradition agreement with the US, did violate Soering's human rights in light of the death penalty prosecution).

330. *Id.*

331. ECHR, *supra* note 80, art. 35.

332. Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security of 9 Dec. 2011, 2012 O.J. (C 35) 16.

333. *Id.* at 18.

United States. The fallout from this was that, through the EU-US PNR agreements, the fundamental rights to privacy and data protection of citizens of the EU were put at risk. The entry into force of the Treaty of Lisbon further strained the EU-US PNR dialogue by reinforcing and enhancing the rights of the EU citizenry. The ultimate result is that, since none of the agreements or proposed agreements fit within the EU legal framework and since the United States is unwilling to budge, meaning negotiate, or compromise, a stalemate between the United States and the European Parliament looms.

From the inception of the ATSA and thereby the EU-PNR dialogue, the United States has dominated the negotiations while the European Commission has more or less simply accepted the terms presented.[334] The EU, arguably, is the last political and legal check on the United States and its seemingly global-reaching domestic policies.[335] If the EU is not willing to stand their ground and instead buckles to US pressure, the landscape of global privacy and data policy will most certainly tilt almost wholly to the US perspective. At the risk of destroying this last line of defense against a US policy regime, the EU must make the United States meet EU terms and fit a new PNR agreement within the laws of the EU. Additionally, recent changes in the primary foundational law of the EU through the Treaty of Lisbon have made it impossible for the EU to maintain the status quo approach to EU-US PNR agreements. An agreement which does not fall within the legal framework of the EU risks annulment by the ECJ or, perhaps even more detrimentally, the ECtHR striking down the agreement on human rights grounds.[336] In this period of change and flux, one thing is certain, the EU cannot meet all of the US demands for terms of a PNR agreement and at the same time abide by their own domestic law meaning that there must be some compromise by the United States.

The post-9/11 US transportation policy, in the context of PNR, is for the security of air travel within, to, or from the United States, but structuring an agreement that fits within EU standards does not mean that the United States downgrades its security. Some critics argue that the EU has no right to push their privacy and data protection standards on the United States.[337] However, is the United States not doing just that by forcing their domestic law and policy regarding PNR on the EU? What the United States is actually doing is pushing off the expenses and resources of border security onto other nations.[338] The United States can still gain an appropriate and ample amount of PNR from the EU and meet the other EU standards all without risking national security if it simply increased other

334. Travis, *supra* note 26.
335. Rasmussen, *supra* note 59, at 589.
336. Guild & Brouwer, *supra* note 88, at 4.
337. McNamara, *supra* note 23.
338. Rasmussen, *supra* note 59, at 590.

mechanisms of border control such as increased visa requirements or requiring data disclosure at its borders.[339] Whatever the outcome of the current EU-US PNR situation, the result will undoubtedly have an extensive influence and bearing on the transmission of data, its protection, and the privacy of individuals throughout the world.

339. *Id.*