NOTE

NO MAN'S LAND:

THE E.U.-U.S. PASSENGER NAME RECORD AGREEMENT
AND WHAT IT MEANS FOR THE EUROPEAN UNION’S
PILLAR STRUCTURE

Christopher Patton*

INTRODUCTION

On August 10, 2006, London police successfully stopped a group of terrorists plotting to use liquid explosives to bomb nine planes flying from the United Kingdom to the United States.1 The plotters had hoped to set off these explosives mid-flight, killing an estimated 2,700 passengers.2 Several weeks after the arrests, U.S. Department of Homeland Security Secretary Michael Chertoff wrote an op-ed in the Washington Post in which he claimed that these terrorist plots failed “precisely because of timely, actionable intelligence, properly shared and acted upon before the terrorists could carry out their plans.”3 He noted that one investigative resource essential to continued success in this area was passenger name record (PNR) data, information, gathered by airlines and travel agencies, which include such valuable clues as “travel itineraries and payment details.”4 Chertoff then lamented that despite agreements with European partners, the United States remained “handcuffed in our ability to use all available resources to identify threats and stop terrorists.”5

Chertoff’s comments were well-timed since only two months earlier the European Court of Justice (ECJ) had struck down the 2004 agreement between the European Union and the United States

2. Id.
3. Michael Chertoff, A Tool We Need to Stop the Next Airliner Plot, WASH. POST, Aug. 29, 2006, at A15.
4. Id.
5. Id.
regarding the processing and transfer of passenger name record data (2004 PNR Agreement).\footnote{6} While Chertoff sought a new agreement that would free the U.S. Department of Homeland Security (DHS) from bothersome data privacy protections, his E.U. counterparts confronted very different concerns regarding the new accord. These concerns were due in part to the increasing outcry among European citizens over the United States’ perceived mishandling of personal data. Such concerns about privacy, however, paled in comparison to the more fundamental questions of structural authority that arose out of the ECJ’s decision to invalidate the agreement.

Signed in 1992, the Treaty on European Union (TEU) established the legal framework of the European Union as it exists today.\footnote{7} This framework grants the European Union authority to act in three distinct areas of competence, or “pillars.”\footnote{8} Each pillar delineates a set of policy areas over which the European Union has authority, and each creates a unique set of procedures for governmental action. The First Pillar grants the European Union authority to regulate commercial and economic affairs.\footnote{9} The Second Pillar enables member states to cooperate in the area of foreign and security policy.\footnote{10} The Third Pillar authorizes “common action among the Member States in the fields of police and judicial cooperation in criminal matters.”\footnote{11}

As the institution charged with approving international agreements between the European Union and third countries, the Council of Europe claimed that the First Pillar—the pillar governing commercial and economic matters—granted them the authority to conclude the 2004 PNR Agreement.\footnote{12} The Council’s rival institution within the E.U. governmental structure, the European Parliament, felt that the agreement was inadequate, both pro-
cedurally and substantively, and, in response, brought an action in the ECJ challenging the 2004 PNR Agreement on four grounds, including that the Council lacked the authority under the First Pillar to make the agreement, and that the agreement infringed on fundamental rights of privacy. On May 30, 2006, the ECJ announced its decision to invalidate the 2004 PNR Agreement. Surprisingly, its opinion ignored the issue of privacy rights altogether, and instead focused on the more fundamental issue of the European Union’s authority to enter into such an agreement in the first place. In its opinion, the ECJ held that the European Union’s power to regulate commercial affairs did not enable it to make such agreements. 

Essentially, the ECJ said that if E.U. officials wanted to enter into a valid PNR agreement with the United States, they would have to find another source of authority.

On October 16, 2006, a temporary agreement (2006 PNR Agreement) was signed which, in turn, was replaced with a similar, but permanent, PNR agreement in August 2007 (2007 PNR Agreement). Despite Chertoff’s efforts, the 2006 and 2007 PNR Agreements contained few substantive changes from the 2004 version. One aspect, however, was different: while the 2004 PNR Agreement’s language focused on the commercial aspects of data transfers between the airlines and the U.S. government, the language of the new agreements asserted that their purpose was “to prevent and combat terrorism and transnational crime effectively as a means of protecting . . . democratic societies and common values.”

This shift in language between the 2004 PNR Agreement and the 2007 PNR Agreement was significant because it signaled a change in the agreement’s legal foundation. No longer able to rely on the First Pillar as legal authority, E.U. officials placed this new emphasis on national security to invoke Third Pillar authority—the pillar

14. See id. ¶ 70.
15. See id. ¶ 67.
which grants the European Union the power to oversee police and judicial cooperation in criminal matters. In other words, the European Union responded to the ECJ’s judgment by basing the 2007 PNR Agreement on a new source of legal authority.

Part I of this Note will discuss the procedural and historical background leading up to the 2007 PNR Agreement. Part II will examine the European Union’s Third Pillar authority. Part III will argue that the 2007 PNR Agreement cannot be based on the Third Pillar, and thus falls into a “no-man’s land” of legal authority that the European Union’s pillar system is ill-equipped to handle.

PART I

A. The European Union’s Data Privacy Directive

The European Union’s Data Privacy Directive is considered one of the most “ambitious and far-reaching data privacy initiatives of the high-technology era.”18 The Data Privacy Directive is rooted in one of the European Union’s fundamental purposes: “to ensure the economic and social progress of [the European] countries by common action to eliminate the barriers which divide Europe.”19 Because the European Union sees parity between member states’ data protection standards as essential to enhanced cross-border commerce, the European Union enacted the Data Privacy Directive to regulate the commercial transfer of personal data among European countries.20 According to its preamble, the Data Privacy Directive exists so “Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedom of individuals, and in particular the right to privacy.”21

The Data Privacy Directive’s scope is broad, requiring member states to establish stringent data protection standards for the “processing of personal data”22 that occurs as a part of any com-

---

19. EC Treaty pmbl.
21. Id. pmbl. (9). Within the limits established in the Data Privacy Directive, the measure calls for Member States to enact their own laws to ensure that the goals of the Data Privacy Directive are met and to “determine more precisely the conditions under which the processing of personal data is lawful.” Id. art. 5.
22. Id. art. 3(1). Processing includes, among other things, “collection, recording, organization, storage . . . alteration, retrieval, consultation, use . . . dissemination . . . blocking, erasure or destruction.” Id. art. 2(b). The Data Privacy Directive also defines “personal
mmercial activity covered by the European Union’s First Pillar authority. But the Data Privacy Directive also delineates several exceptions to these restrictions, the broadest of which excludes the processing of data in “any case . . . concerning public security, defense, state security (including the economic well-being of the state when the process operation relates to state security matters) and the activities of the state in areas of criminal law.”

An essential aspect of the Data Privacy Directive’s success has been its regulation of data transfers to countries outside the European Union. Articles 25 and 26 of the Data Privacy Directive establish explicit standards and procedures for such transfers, stating that member states may only allow personal data to reach third countries if “the third country in question ensures an adequate level of protection.” The Data Privacy Directive further requires the European Commission, a unit of the European Union that often functions as the executive branch, to examine “all the circumstances surrounding a data transfer operation” with particular attention paid to “the nature of the data, the purpose and duration of the proposed processing operation(s), the country of origin and country of destination, [and] the rule of law” to determine whether a third country’s data protection standards are adequate. Only after the Commission makes a finding that the third country in question ensures adequate protection will data transfers be permitted. If, however, a third country does not meet the Data Privacy Directive’s requirements for data protection, the Commission must ensure that member states take measures to stop the transfer of data to that country.

B. The Aviation and Transportation Security Act of 2001

In November 2001, the U.S. Congress passed the Aviation and Transportation Security Act, which included, among many other...
things, a provision requiring all foreign air carriers flying into or over the United States to provide the Commissioner of Customs with specific passenger and crew manifest information. The act also empowered the secretary of transportation to promulgate regulations clarifying and supplementing these requirements. Shortly thereafter, the U.S. Department of Transportation issued regulations requiring all commercial aircraft arriving in the United States from a foreign country to “transmit to [Customs and Border Protection systems] an electronic passenger arrival manifest covering any passengers on board the aircraft.” According to the regulation, the transmission of this information must occur no later than 15 minutes after the departure of the aircraft. The regulations also specified the categories of information that the airlines must transmit, including the following: each passenger’s name; date of birth; gender; citizenship; country of residence; status on board the aircraft; travel-document type; passport number; passport country; passport expiration date; alien registration number; and address while staying in the United States.

C. The 2004 PNR Agreement

In response to the conflicting requirements of the Data Privacy Directive and the Aviation and Transportation Security Act, the European Union and the United States sought a compromise. The goal was to establish an agreement that would enable foreign airlines to fly into and out of the United States without violating the law on either side of the Atlantic. Before a treaty could be signed, however, E.U. officials had to take the steps prescribed by the Data Privacy Directive to determine whether U.S. data protection standards were adequate. Pursuant to Article 25(6) of the Data Privacy Directive, the European Commission evaluated U.S. privacy standards and determined that the U.S. Bureau of Customs and Border Protection (CBP) provided an adequate level of protection for the PNR data to be transferred from European airlines to the United States. This adequacy decision turned largely on the United

States’ agreement to abide by a specific set of standards it had outlined in a document called “Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection” (Undertakings) which it had submitted to the Commission.\[^{36}\]

The final 2004 PNR Agreement bore the title “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” and contained little in terms of substantive data protection measures.\[^{37}\] Its provisions, however, made clear that the agreement’s validity under the Data Privacy Directive rested wholly upon the CBP’s compliance with the above-mentioned Undertakings.\[^{38}\] The agreement also enabled CBP to have direct electronic access to European airlines’ databases.\[^{39}\] This method of access, called the “pull” system, was granted out of practical necessity, and the agreement established that such a system would prevail “only until there is a satisfactory system in place allowing for transmission of such data by the air carriers.”\[^{40}\] The agreement’s other provisions required a joint and regular review of the agreement\[^{41}\] as well as an acknowledgment that the United States would allow the European Union to receive PNR informa-

\[^{36}\] Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41,543, 41,543-45 (July 9, 2004) [hereinafter Undertakings Regarding PNR]. This set of undertakings established a number of limitations on U.S. Bureau of Customs and Border Protection’s (CBP’s) use of this PNR data. In the most crucial of these limits, CBP agreed to use PNR data only for preventing or combating: (1) terrorism; (2) other serious crimes, including organized crime; and (3) flights from warrants or custody the above two crimes. See id. CBP also agreed to “pull passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to push the data to CBP.” Id. at 41,544. This distinction is important because it enabled CBP to have direct access (that is, to reach in and pull information directly from the airline’s databases). Such a feature gives the CBP access to “airline data without filters for sensitive information or for non-transatlantic flights.” Council Decision Regarding Agreement Between The Europe An Community And The United States On The Use Of Passenger Name Record Data, 11 COLUM. J. EUR. L. 207, 211 (2004). Finally, CBP agreed to limit access to data by only allowing “certain CBP officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data.” Undertakings Regarding PNR, 69 Fed. Reg. at 41,545.

\[^{37}\] See 2004 PNR Agreement, supra note 12.

\[^{38}\] See id. ¶ 3.

\[^{39}\] See id. ¶ 1.

\[^{40}\] Id.

\[^{41}\] Id. ¶ 5.
tion from U.S. airlines should it enact a similar requirement in the future.\textsuperscript{42}

Significantly, the European Council entered into the agreement on the basis of its First Pillar authority as laid out in Article 95 of the Treaty establishing the European Community (TEC).\textsuperscript{43} This article allows the Council to enact legislation that has as its “object the establishment and functioning of the internal market.”\textsuperscript{44} In other words, the legal foundation of 2004 PNR Agreement rested on the European Union’s authority to regulate commercial activity. The First Pillar provides the Council with the most comprehensive regulatory power of any of the pillars, enabling the Council to act supra-nationally—in some cases by the means of a simple majority.\textsuperscript{45}

D. Parliament’s Challenge to the 2004 PNR Agreement

The European Council, however, failed to involve the European Parliament when it defined the substance of the 2004 PNR Agreement.\textsuperscript{46} Parliament, frustrated with the Council’s unilateral activity, challenged the 2004 PNR Agreement’s legality in the ECJ, taking issue with both the Council’s decision to enter into the agreement as well as the European Commission’s determination regarding the adequacy of the U.S. data protection standards.\textsuperscript{47} Parliament’s primary contention was that Article 95 of the TEC did not grant the Council authority to make such an agreement.\textsuperscript{48} It

\textsuperscript{42} See id. ¶ 6.


\textsuperscript{44} EC Treaty art. 95.

\textsuperscript{45} See, e.g., EC Treaty art. 300.

\textsuperscript{46} During negotiations, the Council of Europe attempted to consult with the European Parliament, as required by Article 300(3) of the Treaty establishing the European Community. Parliament did not, however, get back to the Council in time to have any significant input into the agreement. See Council Decision 2004/496/EC, 2004 O.J. (L 183/83) ¶ 2. For a number of reasons, Parliament was not happy with the agreement. Some of these reasons stem from changes in the balance of power within the European Union itself, but others represent an increasing concern about privacy among Parliament’s electorate.


\textsuperscript{48} See id. ¶ 63.
further argued that both the Commission’s and the Council’s actions infringed fundamental privacy rights.\(^{49}\)

In a terse opinion, the ECJ found that both the agreement itself and the decision on adequacy had no valid legal basis.\(^{50}\) The ECJ reasoned that because the Data Privacy Directive does not specifically cover issues of national security or public safety, its provisions were not applicable in this case.\(^{51}\) The ECJ further held that Article 95 of the TEC, which provides authority for the Council to act in the area of commercial regulation, does not grant the Council authority to enter into an agreement of this type, and stated instead that “the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law.”\(^{52}\) Finally, the ECJ noted that because the 2004 PNR Agreement and adequacy decision were not legally valid, the issue of whether they infringed fundamental rights of privacy was moot.\(^{53}\)

Because the ECJ acknowledged that the absence of an agreement in this area would generate significant operational issues for airline companies, it determined that the 2004 PNR Agreement would remain in effect until September 30, 2006, allowing time for the European Union and the United States to establish a replacement agreement based on a proper legal foundation.\(^{54}\)

---

49. See id.
50. See id. ¶¶ 61, 70.
51. See id. ¶ 68.
52. See id. ¶ 56 (emphasis added).
53. See id. ¶ 61. The European Court of Justice (ECJ) decision to forego discussing whether the agreement infringed on fundamental privacy rights was significant given Advocate General Phillipe Léger’s preliminary opinion which discussed the matter thoroughly. Léger discussed extensively whether, regardless of its validity, the agreement infringed on the right to protection of personal data. See Opinion of AG Léger, Joined Cases C-317 & C-318/04, Parliament v. Council & Parliament v. Comm’n, 2006 E.C.R. I-4721, ¶¶ 193-268. To begin, he noted that Article 8 of the European Convention on Human Rights creates a right among European citizens to the protection of personal data. See id. ¶ 208. Léger then discussed thoroughly whether the Council of Europe’s conclusion of the agreement or the European Commission’s decision on adequacy infringed on this right. See id. ¶¶ 215-62. The law in this area, he concluded, was clear: “[I]n order to be permissible, interference in private life must be found to satisfy three conditions. It must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society.” Id. ¶ 214. In this case, each of these conditions was satisfied. First, the undertakings of the CBP were extensive enough such that the agreement was “in accordance with the law.” Id. ¶ 221. Second, national security concerns were sufficient to establish that the agreement was in pursuance of a “legitimate aim.” Id. ¶ 223. Third, the agreement was “necessary in a democratic society” because it was proportional to the potential harm involved. Id. ¶ 262. Thus, if the agreements and decisions on adequacy were based on a proper foundation, they would not infringe on the fundamental right to privacy.
E. The 2006 and 2007 E.U.-U.S. PNR Agreements

While the ECJ’s decision was a nominal victory for the European Parliament, many observers were rattled by the implications of the decision. One of the most prominent data protection authorities in Europe, the European Data Protection Supervisor, noted that the decision “seem[ed] to create a loophole in the protection of the European citizen since it is no longer assured that data collected for commercial purposes but used by police [were] protected by the data protection directive.”\(^\text{55}\) Parliament also had a strong reaction to the decision. Despite the fact that the new agreement would be made under treaty provisions which strongly limited Parliament’s powers, many members of Parliament asserted that Parliament should play a central role in the development of the new agreement.\(^\text{56}\)

While the language of the 2004 PNR Agreement centered around the commercial aspects of data transfers between airlines and the U.S. government, this 2006 PNR Agreement—concluded shortly after the ECJ imposed deadline—stated a starkly different mission: “to prevent and combat terrorism and transnational crime effectively as a means of protecting . . . democratic societies and common values.”\(^\text{57}\) Furthermore, the words “public security,” “law enforcement,” and “terrorism” appeared numerous times in this replacement agreement.\(^\text{58}\) Such language indicated a shift in the agreement’s legal foundation from the First Pillar to the Third Pillar. Beyond these changes, however, the 2006 PNR Agreement was almost identical to its predecessor.\(^\text{59}\)

In July 2007, a permanent PNR agreement replaced the 2006 version. Like its predecessor, this revision contained few substan-

---


\(^\text{56}\) Shortly after the decision, the President of the European Parliament sent letters to the Council of Europe and the European Commission requesting that Parliament “should fully be kept involved in the process aiming at the replacement of the annulled decisions.” Letter from Fontelles to Barroso and Schussel (June 6, 2006). The Council and Commission, however, were reluctant to include Parliament, with a commission spokesman noting that “[u]nder the procedure there is no formal role for the parliament to play.” Bruno Waterfield, MEPs to Be Snubbed in New EU-US Air Data Deal, PARLIAMENT, June 19, 2006, http://www.europolitix.com/EN/News/200606/15eeede6-4755-4b14-9ebc-68b6d4e864a.htm.

\(^\text{57}\) 2006 PNR Agreement, supra note 16.

\(^\text{58}\) Id.

\(^\text{59}\) See id. ¶ 7. One final difference between the two agreements established that the 2006 PNR Agreement was only temporary and would expire on July 31, 2007. See id. ¶ 7.
tive changes from the initial agreement struck down by the ECJ. But unlike the original 2004 PNR Agreement, the 2007 PNR Agreement, similar to the 2006 PNR Agreement, focused its language on terrorism and transnational crime, indicating that it too would claim the Third Pillar as its authority.

PART II

A. The European Union’s Pillars of Legal Authority

To understand what the 2007 PNR Agreement contributes to the European Union’s changing structure, it is first necessary to examine more fundamental notions of legal authority. The European Union is the creation of a number of treaties, some going back as far as 1952. Until the TEU in 1992, the European Union’s authority to legislate centered almost exclusively on economic and commercial affairs. In 1992, Member States came together to create a method for cooperation in matters of foreign policy and “home affairs.” The treaty that emerged, known as both the TEU and the Treaty of Maastricht, created the European Union as it exists today.

The treaties creating the European Union “may be viewed as making up the EU’s political constitution.” Just as the U.S. Constitution delegates to the federal government authority to act in only specified arenas, the TEU grants the European Union the power to act only in limited spheres of authority. Thus, any action taken by the European Union must ultimately stand on authority granted to it by one of the three pillars.

Under the First Pillar, the European Union retained much of its previous power to regulate internal commercial and economic affairs. The First Pillar is a commonly used source of authority, in part because it allows the European Union to act without unanimous consent from all the member states. Because of this, the First Pillar is “by far the most important pillar since it incorporated

61. See id. at 49, 82-93. Pre-TEU, the European Union only regulated the internal market and was called the European Community. The TEU “created the new organization of the European Union, which was based on three pillars.” Id. at 49.
62. See id.
63. See id.
64. Id. at 283
65. See id. at 86.
66. See id.
most of the European Union’s policy responsibilities.”67 From a data privacy perspective, the First Pillar also contains the most comprehensive privacy protections in the form of the Data Privacy Directive, which does not apply to the Second or Third Pillars.68

The Second Pillar created a system to manage a joint foreign and security policy.69 The TEU established that “the EU and its member states ‘shall define and implement a common foreign and security policy . . . covering all areas of foreign and security policy,’ and by further specifying that the common policy ‘shall include all questions related to the security of the Union, including the eventual framing of a common defense policy, which might in time lead to a common defense.’”70 This Pillar is “considered the least developed flank of Community integration and, consequently, one of its weakest points.”71 This is due, in part, to inconsistencies inherent in the E.U. constitutional structure which have led to a system that allows foreign policy action under all three pillars.72

B. The European Union’s Third Pillar Authority

The Third Pillar focuses on member state cooperation in the area of law enforcement and judicial matters.73 In its original form under the TEU, the Third Pillar bore the title “Justice and Home Affairs” and comprised a number of controversial policy areas—everything from asylum and immigration policy to police cooperation in combating terrorism, drugs, and xenophobia.74 To add to this broad policy portfolio, the TEU also strongly limited the European Union’s power to act in each of these areas.75 For example, every action taken under the Third Pillar had to receive unanimous consent from member states, and even when that consent existed, the allowable range of potential action was extremely nar-

67. Id.
69. See Nugent, supra note 60, at 89.
70. Id. at 89.
72. One observer has noted that “the attempt to delineate between the Community’s external competences regarding international trade and the European Union’s competences regarding international order and security is anomalous and clumsy.” Ian Ward, The Challenges of European Union Foreign and Security Policy: Retrospective and Prospective, 15 TUL. J. INT’L & COMP. L. 5, 12 (2005) (internal quotations omitted).
73. See Nugent, supra note 60, at 90-91.
74. See id.
75. See id. at 91.
row. Perhaps the primary obstacle impeding effective Third Pillar action was that it regulated matters over which many member states were unwilling to give up decision-making power.

The Treaty of Amsterdam, signed in 1997, strengthened the Third Pillar in a number of ways. First, it transferred many of the more controversial policy areas, including immigration and asylum matters, to the First Pillar. This newer, narrower focus was reflected in the new name the Third Pillar was given by the Treaty of Amsterdam: “Provisions on Police and Judicial Cooperation in Criminal Matters.” Its post-Amsterdam mission would be to provide citizens “with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia.” The Treaty of Amsterdam also helped increase the Third Pillar’s effectiveness by giving the ECJ greater, though still somewhat limited, jurisdictional power.

Since 1997, the Third Pillar has undergone relatively few changes. Recently, several anti-terrorist measures were added, including a European Union–wide arrest-warrant procedure intended to replace extradition proceedings. Given the increasing focus on national security, it is not surprising that the Third Pillar has received much attention of late. One observer noted that “there is no other example . . . of an area of loose intergovernmental cooperation having made its way so quickly to the top of the Union’s political and legislative agenda.”

**PART III**

Though procedural requirements precluded the European Parliament from extensive involvement with the 2006 PNR Agreement, members of Parliament nonetheless debated the issue vigorously. The rhetoric in these debates revealed several interesting positions. One member of Parliament, Johannes Vog-
genhuber, made the following observation regarding the 2006 PNR Agreement: “Today we are looking at an agreement under the III pillar, no public debate, no role of [European Parliament], no ratification of national parliaments . . . it continues to be a transfer of data outside the protection of the law.”

Though Voggenhuber may not have realized it at the time, his comment highlighted an important problem with the new agreements: the 2006 and 2007 PNR Agreements, like the 2004 PNR Agreement, was based on a shaky legal foundation. Indeed, a close look at the 2007 PNR Agreement reveals a “no-man’s land” of legal authority in the European Union’s pillar system—a fundamental flaw which fails to provide the European Council with the legal authority necessary to conclude any agreement of this type.

A. The 2004 PNR Agreement and the First Pillar

The 2004 PNR Agreement was based on Article 95 of the TEC, which enables the European Union to adopt measures, including international agreements with third countries, that seek to enhance the “internal market.” As discussed above, the ECJ struck down the 2004 PNR Agreement because it had little to do with the internal economic matters mentioned in Article 95. While the ECJ’s opinion in the PNR case did not cite prior decisions to buttress its conclusion, the ECJ’s previous opinions fully support its decision to invalidate the agreement.

The ECJ has held that “the choice of the legal basis for a Community measure must rest on objective factors which are amenable to judicial review, including in particular the aim and the content of the measure.” Its case law has further established that to

86. EC Treaty art. 95.
88. The ECJ does not employ the common law doctrine of stare decisis. In practice, however, prior decisions are quite relevant to the ECJ. See Louis F. Del Duca, Developing Global Transnational Harmonization Procedures for the Twenty First-Century: The Accelerating Pace of Common and Civil Law Convergence, 42 Tex. Int’l L.J. 625, 647-48 (2007) (“Although precedent is not a formal source of ECJ law, the Court often specifically refers to prior decisions and advocates cite cases freely in written briefs and during the oral stage of the proceeding.”). This notion is confirmed by the Advocate General’s statements that “the Court should, as a matter of practice, follow its previous case-law except where there are strong reasons for not doing.” Joined Cases C-267/95 & C-268/95, Merck v. Primecrown, Ltd., 1996 E.C.R. I-6285, 6344.
ground legislation in First Pillar authority, the aim and content of the measure must be “intended to improve the conditions for the establishment and functioning of the internal market and must genuinely have that object, actually contributing to the elimination of obstacles to the free movement of goods or to the freedom to provide services, or to the removal of distortions of competition.”

According to the ECJ, the fact that an action has incidental effects on the internal economy alone does not satisfy this requirement.

Given such precedent, the ECJ was correct to find that the 2004 PNR Agreement lacked the proper legal basis. Although the PNR data was itself commercial data, the agreement was not commercial in nature. Indeed, preamble to the 2004 PNR Agreement noted “the importance of . . . preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime.” And as the ECJ rightly found, the 2004 PNR Agreement’s references to commercial matters were few and incidental to its overall purpose. Indeed, the only direct reference to First Pillar matters that appeared in the European Council Decision authorizing the signing of the agreement noted that the European Parliament was excluded from the negotiations because of the relative uncertainty that the European airlines and passengers encountered “as well as to protect the financial interests of those concerned.”

B. The 2007 PNR Agreement and the Third Pillar

At first glance, the 2007 PNR Agreement appears to fit perfectly with the Third Pillar’s objective of “preventing and combating crime . . . in particular terrorism.” A closer look at the peculiar circumstances surrounding this type of data transfer, however, reveals a much more complicated scenario. In particular, the fact that these PNR transfers occur between private corporations and third countries like the United States jeopardizes the 2007 PNR Agreement’s ability to rest soundly on Third Pillar authority.

90. C-491/01, British American Tobacco (Invs.) Ltd. & Imperial Tobacco, 2002 E.C.R. I-11453, ¶ 60.
91. See C-426/93, Germany v. Council, 1995 E.C.R. I-3723, ¶ 33 (“[T]he mere fact that an act may affect the establishment or functioning of the internal market is not sufficient to justify using that provision as the basis for the act.”).
92. See, e.g., C-491/01, British American Tobacco (Invs.) Ltd. & Imperial Tobacco, 2002 E.C.R. I-11453, ¶ 60.
93. 2004 PNR Agreement, supra note 12, pmbl.
95. TEU, supra note 7, art. 29.
C. Title VI of the TEU and the 2007 PNR Agreement

The language of Title VI of the TEU implies that measures enacted pursuant to this authority only govern actions among member states.96 Article 29 sets forth the Third Pillar’s fundamental purpose: to “provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters.”97 According to the TEU, member states should seek to meet this objective “by preventing and combating crime . . . through [(1)] closer cooperation between police forces, customs authorities and other competent authorities in the Member States . . . [(2)] closer cooperation between judicial and other competent authorities of the Member States . . . [and (3)] approximation, where necessary, of rules on criminal matters in the Member States.”98 More particularly, closer cooperation in criminal matters can be achieved through “operational cooperation between the competent authorities” and “the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol.”99

The 2007 PNR Agreement’s language establishes a system that regulates the transfer of information from private corporations to the law enforcement authorities of a third country—in this case, DHS. The private corporations involved in these transfers are hardly the “competent authorities” and “police forces” that Article 29 envisions.100 Moreover, the 2007 PNR Agreement does not foreshadow a time when European airlines will transfer their PNR data to member states who will, in turn, transfer that data to the United States—a method of transfer that would perhaps more appropriately fall within the Third Pillar framework.101 According to the


97. TEU, supra note 7, art. 29 (emphasis added).

98. Id.

99. Id., art. 30(a)-(b).

100. See Hijmans, supra note 96, ¶ 36 (“Such activities by private firms in connection with the performance of criminal law tasks cannot simply be brought within the scope of the Third Pillar.”).

101. See 2007 PNR Agreement, supra note 16, ¶ 2 (“DHS will electronically access the PNR from air carriers’ reservation systems located within the territory of the Member
2007 PNR Agreement, the only role that the European Union is to play in these data transfers is to “ensure that air carriers with reservation systems located within the European Union make available PNR data to DHS and comply with the technical requirements for such transfers as detailed by DHS.”

Foreseeing this problem, both the ECJ in its judgment on the 2004 PNR Agreement and Advocate General Phillippe Léger in his opinion on the same matter attempted to defuse the contention that any subsequent PNR agreement would be a square peg in the Third Pillar’s round hole. The ECJ briefly noted that even though the PNR data was collected and transferred by private corporations, “[t]he transfer falls within a framework established by the public authorities that relates to public security.” Léger’s opinion dug much deeper into the “tricky question” of whether a replacement PNR agreement could exist under the Third Pillar. Léger first observed that, for Third Pillar purposes, any action undertaken to supply a third country with personal data intended to protect its internal security should qualify as cooperation between public authorities. He then claimed that “requiring a legal person to undertake such processing of data and obliging it to transfer those data does not seem to . . . be fundamentally different from a direct exchange of data between public authorities.”

The problem with both opinions, however, is that neither attempted to provide any sort of rationale to support its sweeping characterization of Third Pillar authority. Léger readily admits that this “case actually concerns a new set of issues,” but fails to present any argument besides blanket assertions. In his view, it is self-evident that Lufthansa Airlines allowing DHS to access its servers constitutes the same thing as the United Kingdom transferring its homegrown anti-terrorist information to the FBI. Several considerations suggest that Léger’s contention is incorrect and

States of the European Union until there is a satisfactory system in place allowing for the transmission of such data by the air carriers.”

102. See id. pmbl.
103. Joined Cases C-317/04 & C-318/04, Parliament v. Council and Comm’n, 2006 E.C.R. I-4721, ¶ 58. The ECJ did not explicitly address whether the Third Pillar would constitute the proper legal foundation in this situation, and this quote comes within the discussion determining merely that the Data Privacy Directive’s “public security” exception does not apply.
105. Id. ¶ 159.
106. Id. ¶ 160.
107. Id.
that the Third Pillar is instead as ill-equipped to support the 2007 PNR Agreement as the First Pillar was to support the 2004 PNR Agreement.

D. The Framework Decision for Data Protection under the Third Pillar and the 2007 PNR Agreement

The Third Pillar’s inability to support the 2007 PNR Agreement becomes apparent when compared with other Third Pillar measures attempting to regulate the transfer of law enforcement data to third countries. Commercial data transfers to third countries under the First Pillar must conform to the comprehensive standards of the Data Privacy Directive. When data transfers relate to Third Pillar criminal and anti-terrorist activities, however, parties are not required to meet any pre-determined privacy standards. For this reason, a solution was recently debated by E.U. officials involving the transfer of police data among member states and to third countries.

In the past few years, the European Union has sought to facilitate the exchange of law enforcement information among member states on the principle that “information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States.” Successful implementation of this principle, however, required uniform Third Pillar data protection standards regarding the retransmission of that data to countries outside the European Union because “Member States will only fully trust each other if there are clear and common rules for the possible further transmission of exchanged data to other parties.” In 2005, the European Commission proposed that crime-related data transfers to non-member states be regulated as part of a comprehensive framework governing data protection in the Third Pillar, a framework akin to the First Pillar’s Data Privacy Directive.

---

113. See Proposal for Framework Decision, supra note 110, art. 15, ¶¶ 12,13.
The Commission began the process of establishing these standardized levels of data protection for the Third Pillar when it adopted the Proposal for a Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (Framework) in October 2005. The Framework’s main priority, which goes far beyond the scope of this Note, was to establish common data protection standards for the transfer of law enforcement information between member states. But the Framework also included a provision regulating the transfer of information to third countries and international bodies. This provision, originally embodied in Article 15 of the Framework, would apply when member states transferred “personal data received from or made available by the competent authority of another Member State” to third countries such as the United States. In other words, the Framework would regulate what member states can do with the data they receive from other member states. It would impose no data protection standards on those member states who choose to transmit their homegrown information to countries outside the European Union.

The European Council issued its most recent draft of this proposal in December 2007, but since this issue has engendered considerable discussion, it is unclear when, and in what form, the final result will appear. Nevertheless, if what emerges from these deliberations approximates the most recent draft, this Framework, together with the 2007 PNR Agreement, exposes a striking weakness in Third Pillar authority.

First, “the relationship between [the Framework] and ad hoc data protection provisions in other EU instruments” is an “outstanding question[].” The president of the Council has suggested that

114. See id. art. 15, ¶ 1.
115. See id. art. 15, ¶ 2.
116. Id. art. 15.
117. Id.
118. Thus, under the Framework’s proposed standards, if U.K. law enforcement officials request personal data from Italy under the principle of availability, those same officials cannot then turn around and pass that information on to the United States. If one of the U.K. intelligence agencies possesses its own, homegrown data relating to a suspected terrorist, the agency may pass that information to the United States regardless of whether U.S. data protection measures are adequate under the Framework’s standard.
the Framework should only apply “to those cases in which co-operation takes place in the absence of a treaty basis (i.e. a treaty existing prior to the adoption of the [Framework]).” Further-
more, Commission Vice President Franco Frattini declared that, in
his opinion, the Framework would not apply to the PNR Agree-
ment because “agreements with third countries, will ensure that
security issues are properly addressed through the transfer and
appropriate use of PNR data, while protecting personal data guar-
anteed by Article 8 of the Charter of Fundamental Rights.”

Second, even assuming the Framework successfully establishes
comprehensive Third Pillar data protection standards that would
trump ad hoc protections such as those contained in the 2007 PNR
Agreement, the language of the Framework only deals with trans-
fers by competent authorities of member states. Article 15 states
that “Member States shall provide that personal data received from
or made available by the competent authority of another Member
State are not further transferred to competent authorities of third
countries or to international bodies except if such a transfer is in
compliance with this Framework Decision.” This language
clearly envisions a state-to-state transfer of information. As
discussed above, the data transfers from European airlines to U.S.
authorities regulated by the 2007 PNR Agreement require little, if
any, involvement by E.U. member states. This gap in a supposedly
comprehensive legislative effort emphasizes the anomalous nature
of the 2007 PNR Agreement and its inability to rest comfortably on
Third Pillar authority.

E. The E.U.-U.S. Mutual Legal Assistance Agreement and the 2007
PNR Agreement

Other individual Third Pillar agreements with countries outside
the European Union contrast significantly with the 2007 PNR
Agreement. One of the first international agreements based on

121. Proposal for a Council Framework Decision on the Protection of Personal Data Processed in
st12432.en06.pdf.
122. Id.
123. See Proposal for Framework Decision, supra note 110, art. 15.
124. Id.
Third Pillar authority was the Agreement on Mutual Legal Assistance between the European Union and the United States (MLA Agreement). Among other things, the MLA Agreement provides for the transfer of bank information from member states to the United States “to provide for identification of financial accounts and transactions” in the course of criminal investigations.

While this requirement may superficially resemble those in the 2007 PNR Agreement since it involves the transfer of information from commercial entities to the United States, the MLA Agreement’s language is actually quite different. The MLA Agreement requires the member state itself to “promptly ascertain if the banks located in its territory possess information on whether an identified natural or legal person suspected of or charged with a criminal offense is the holder of a bank account” and then that member state “shall promptly communicate the results of its enquiries to the requesting State.” Under the 2007 PNR Agreement, E.U. officials play a very different role, one limited to ensuring that the airlines arrange for transmission themselves. This oversight is even more limited than it appears since the 2007 PNR Agreement establishes that the United States will simply reach into airline servers and take the information it needs. Unlike the MLA Agreement, which fits squarely within the Third Pillar’s purpose of overseeing the actions of member states, the 2007 PNR Agreement seeks to regulate transfers of business information to third countries for police purposes in a much more problematic way.

F. The Data Retention Directive and the 2007 PNR Agreement

Passed on March 15, 2006, the Data Retention Directive sought to make criminal cooperation between member states easier by standardizing private data storage requirements. The Data Retention Directive responded to the needs of European law-

---

127. Id. art. 4(1)(a).
129. See id. ¶ 2.
enforcement officials who found that previous data-retention requirements hampered their investigations.\textsuperscript{131} Both the Data Retention Directive’s legislative history and its current status cast serious doubts on the legitimacy of the 2007 PNR Agreement’s place within the Third Pillar.

The Data Retention Directive requires private telecommunication and internet providers to retain, for a period of six months to two years, a wide variety of “traffic and location data.”\textsuperscript{132} Internet providers must retain sufficient data to identify the source or destination of a communication as well as the date, time, duration, and type of that communication.\textsuperscript{133} The traffic data must then be made available to law-enforcement authorities “for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.”\textsuperscript{134}

The Data Retention Directive was ultimately passed on the basis of First Pillar authority, but it was proposed as a Third Pillar measure.\textsuperscript{135} A number of factors combined to bring about this change in its legal basis, most of them involving political maneuvering by various E.U. institutions.\textsuperscript{136} One observer, however, has noted that the decision to bring the Data Retention Directive under the First Pillar may make sense from a legal perspective, arguing that, although the Data Retention Directive’s principal aim was criminal in nature, “by standardizing the data retention requirements imposed on electronic communications providers by their police authorities, it would be easier for providers to do business in multiple jurisdictions.”\textsuperscript{137}

This argument is weak, however, especially given the ECJ’s holding in \textit{Germany v. Council}, which established that “the mere fact that an act may affect the establishment or functioning of the internal market is not sufficient to justify that provision as the basis for the act.”\textsuperscript{138} Furthermore, it is unclear whether the Data Retention Directive will remain a First Pillar instrument since the government

\begin{itemize}
  \item \textsuperscript{131} For example, the Council Directive on Privacy and Electronic Communications 2002/58/EC, required private companies to erase electronic data as soon as it was no longer need for billing requirements. 2002 O.J. (L 201).
  \item \textsuperscript{132} See Data Retention Directive, supra note 130, art. 1.
  \item \textsuperscript{133} \textit{Id.} art. 5.
  \item \textsuperscript{134} \textit{Id.} art. 1.
  \item \textsuperscript{136} For example, as discussed above, the European Parliament can only “consult” on third-pillar measures. Furthermore, for any measure to pass under the Third Pillar, the Council of Europe would have to act unanimously.
  \item \textsuperscript{137} See Bignami, supra note 130, at 7.
  \item \textsuperscript{138} Case C-426/93, Germany v. Council, 1995 E.C.R. I-3723, ¶ 33.d
\end{itemize}
of Ireland has recently challenged the European Union’s authority to enact the measure under Article 95 of the TEC.\footnote{Action brought on 6 July 2006 — Ireland v. Council of the European Union, European Parliament, Case C-301/06, 2006 O.J. (C 237) 5.}

These challenges to the Data Retention Directive provide further evidence of the problematic nature of the European Union’s pillar system. As with the 2007 PNR Agreement, the Data Retention Directive shows that a clear gap exists within the European Union where measures regulating the use of private data for law enforcement purposes do not fit comfortably within the First or Third Pillar.

\section*{G. Environmental Crimes in the Third Pillar}

At least one argument can be made to support the position that measures governing private firms’ actions in relation to law enforcement activities may indeed have a legal foundation in the Third Pillar. This argument stems from an ECJ decision regarding the validity of a recent Third Pillar measure which provided for environmental protection by requiring member states to adopt criminal penalties for certain acts.\footnote{Council Framework Decision 2003/80/JHA on the Protection of the Environment through Criminal Law, 2003 O.J. (L 29) 55.} This measure was challenged on the basis that the treaty allowing the European Union to engage in environmental regulation rests with the First Pillar, not the Third.\footnote{Case C-176/03, Comm’n v. Council, 2003 E.C.R. I-7879, ¶ 18.} The ECJ found that the measure’s clear objective was to protect the environment and that, despite the fact that it called for criminal penalties, the provision belonged in the First Pillar.\footnote{In making this point, the ECJ recalled the principle that “the choice of the legal basis for a Community measure must rest on objective factors which are amenable to judicial review, including, in particular the aim and the content of the measure.” Case C-300/89, Comm’n v. Council, 1991 E.C.R. I-2867.}

The ECJ then noted that, in general, the First Pillar grants no authority to legislate on criminal matters.\footnote{See id. (“[A]s a general matter, neither criminal law nor the rules of criminal procedure fall within the Community’s competence.”).} Nevertheless, the ECJ made clear that this fact does not prevent the European Union from taking action under the authority of the First Pillar which relates to the criminal law of the member states when necessary to ensure that the rules it lays down on environmental protection are fully effective.\footnote{See id.} This is particularly true when the application of effective, proportionate, and dissuasive criminal penalties by competent national authorities are essential for combating serious envi-
Following this holding, it can be argued that although Third Pillar authority cannot serve as a basis to regulate private entities generally, the European Union can use the Third Pillar to impose on private firms requirements that ultimately serve to achieve the Article 29 goals of closer cooperation in criminal matters. In other words, one argument Advocate General Léger could have made was that the 2007 PNR Agreement legitimately rests on Third Pillar authority because its ultimate goal is to enhance member state cooperation in criminal matters.

But this argument ultimately fails because the case for situating the 2007 PNR Agreement on Third Pillar authority is easily distinguishable from the ECJ's jurisprudence on environmental crimes. In an environmental-crimes case, the ECJ found that the European Union, acting under the First Pillar, can "take . . . measures which relate to the criminal law of Member States" for the purpose of "ensur[ing] that the rules which it lays down on environmental protection are fully effective." Criminal penalties for environmental damage relate to methods of enforcing a law that the European Union already had the authority to make under the First Pillar. In contrast, whether the 2007 PNR Agreement can rest on the authority of the Third Pillar is a question that deals with fundamental issues of legislative jurisdiction. The question is not whether the European Union can pass measures under the Third Pillar which would ensure that other measures within its competence are "fully effective"—rather, the question is whether the primary measure can be passed at all.

**Conclusion**

The choice to ground the 2007 PNR Agreement on Third Pillar authority reveals a fundamental flaw within the European Union's three-pillar constitutional structure. As the ECJ determined, this type of agreement sits clearly outside the boundaries of the First Pillar. But the agreement also fails under the Third Pillar since the 2007 PNR Agreement focuses on interactions between private, European-based corporations and the United States, a third country. Until a European Constitution replaces the beleaguered pillar...
system, this problem will persist and perhaps worsen as counter-terrorism measures require more corporations to hand over the personal data they collect while doing business. For this reason, the 2007 PNR Agreement has broad implications for the European Union’s ability to remain relevant in a time when national security remains a top priority for every government.