



School of Law

HOMELAND SECURITY, INFORMATION POLICY, AND THE TRANSATLANTIC ALLIANCE

**Stewart A. Baker, Center for Strategic and
International Studies; Steptoe & Johnson**

**Nathan A. Sales,
George Mason University School of Law**

**George Mason University Law and Economics
Research Paper Series**

09-20

This paper can be downloaded without charge from the Social Science
Research Network at http://ssrn.com/abstract_id=1361943

Homeland Security, Information Policy, and the Transatlantic Alliance

Stewart A. Baker[†]
Nathan Alexander Sales^{††}

It's June 14, 2003 at Chicago's O'Hare international airport. The U.S.-led war to topple Saddam Hussein's Ba'athist regime in Iraq was launched a little less than three months ago. Resurgent fears of terrorism have kept some would-be passengers from the skies, but O'Hare is still operating at a fairly brisk pace.

A Jordanian man named Ra'ed al-Banna is among the throng of passengers who have just arrived on KLM flight 611 from Amsterdam. After waiting in line, al-Banna presents his passport to U.S. Customs and Border Protection officers. The CBP officers consult the computerized targeting system used to screen passengers who seek to enter the U.S. The information about al-Banna – drawn from his airline reservations and past travel – triggers a closer look. The officers examine al-Banna's documents, and they begin asking him questions.

Something doesn't add up. Al-Banna has a legitimate Jordanian passport; he holds a valid visa that allows him to work in the United States; and he had visited the U.S. before for a lengthy stay. But the officers aren't satisfied that he's being completely truthful with his answers, so they decide to refuse him admission. Al-Banna's fingerprints are taken, and he is put on a plane back to Jordan.

So far it sounds like a fairly routine day at the border. And it was, until events in Iraq nearly two years later gave it a new, and sinister, significance.

On February 28, 2005, at about 8:30 in the morning, several hundred police recruits were lined up outside a clinic in Hilla, a city in the south of Iraq. With no warning, a car drove into the crowd and detonated a massive bomb. 132 people were killed, and about as many were wounded. At the time, it was the deadliest suicide bombing Iraq had seen.

The driver was Ra'ed al-Banna. We know that because when authorities found the steering wheel of his car, his forearm was still chained to it.¹

No one knows why al-Banna wanted to be in the U.S. in 2003, or what he would have done if he had gotten in. But we do know what kept him out – the government's ability to

[†] Distinguished Visiting Fellow, Center for Strategic and International Studies; Partner, Steptoe & Johnson LLP.

^{††} Assistant Professor of Law, George Mason University School of Law. Messrs. Baker and Sales previously served at the U.S. Department of Homeland Security as Assistant Secretary for Policy and Deputy Assistant Secretary for Policy Development, respectively. The opinions expressed in this chapter are those of the authors alone, and do not reflect the views of current or former employers or clients. The authors are grateful to Jeremy Rabkin, Neomi Rao, Paul Rosenzweig, and Mike Scardaville for their helpful and insightful comments. Special thanks to Mark Bass for excellent research assistance.

¹ Charlotte Buchen, *The Man Turned Away*, PBS, Oct. 10, 2006, <http://www.pbs.org/wgbh/pages/frontline/enemywithin/reality/al-banna.html>.

quickly marshal the data that first triggered a closer look, and that the CBP officer later used to question al-Banna closely and to conclude that his answers weren't satisfactory. At the center of that system was airline reservation data, known as Passenger Name Records or "PNR."

In the years since 9/11, a consensus has emerged among American policymakers that a crucial way of preventing future attacks is to ensure that counterterrorism officials have access to new sources of information. A perceived need for better, more accurate, and more comprehensive data has animated virtually every major post-9/11 legislative innovation, from the USA PATRIOT Act of 2001 to the 9/11 Recommendations Implementation Act of 2007.

While this approach commands fairly broad support in the United States, it is not without its detractors – especially among America's traditional allies in Europe. Citing European data privacy norms, some European Union policymakers have tried to restrict the ability of the United States to gather, use, and share data for counterterrorism purposes. It is important not to overstate the magnitude of these transatlantic frictions; Washington and Brussels remain close friends and important strategic partners. Yet neither should the significance of this recent and growing trend be missed. Rather than acknowledging the right of the United States as a sovereign to pursue its own policy objectives, some in Europe have sought to export the Continent's data privacy laws to this country.

This chapter will consider the reasons for, implications of, and possible solutions to this growing rift between Washington and Brussels. Before we can turn to that, it's necessary to have a better understanding of how the government uses data at the border and its legal basis for doing so. Part I discusses the use by the United States (especially by the Department of Homeland Security) of various types of information in its efforts to detect and incapacitate terrorist operatives. Special attention will be paid to DHS's use of airline passenger reservation data. In Part II, we survey the legal authorities under which these activities are carried out. Part III examines the response of European policymakers to American efforts to gather and analyze passenger data and related information. In Part IV, we examine possible explanations for Europe's new enthusiasm for projecting its data privacy values globally, and consider solutions that will preserve both individual privacy and national autonomy.

I. PNR and Homeland Security

Information policy is a central front in the war on terrorism. First, the big picture. Since 9/11, Congress has enacted a number of measures designed to improve the flow of data to and within the government. For example, section 203 of the USA PATRIOT Act of 2001 authorizes the sharing of information acquired during grand jury proceedings and through electronic surveillance.² Section 218 of the same legislation tore down the "wall" that prevented intelligence officers from cooperating with agencies pursuing traditional criminal investigations.³ Likewise, section 202 of the Homeland Security Act of 2002 granted the Secretary of Homeland Security access to "all" information in the government's possession that he deems relevant to

² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, § 203, Pub. L. No. 107-56, 115 Stat. 272, 279 (2001).

³ *Id.* § 218, 115 Stat. at 291; *see also In re: Sealed Case*, 310 F.3d 717 (FISCR 2002).

terrorist threats against the United States.⁴ And the Intelligence Reform and Terrorism Prevention Act of 2004 comprehensively restructured the U.S. Intelligence Community, including by creating an “Information Sharing Environment” intended to facilitate the sharing of data among federal, state, and local players.⁵

Why has Congress devoted so much effort to reforming national security information policies? Because information – especially about the tiny handful of terrorist suspects trying to hide in a flood of travelers – allows a targeted response to the challenge of terrorism. Without good data, the U.S. is stuck playing defense. And that’s an expensive proposition. A dollar spent hardening a target against terrorist attack – say a nuclear power plant – will make that particular facility marginally more secure. But it does nothing to protect the nearby oil pipeline or skyscraper. By contrast, spending that same dollar to upgrade data collection and analysis capabilities better enables the government to detect and disrupt any number of terrorist plots.⁶ In other words, Congress reasonably concluded that investments in information policy reform would produce greater returns (measured in overall security against terrorist attacks) than investments in the security of individual potential targets.

One of the most crucial types of information available to counterterrorism officials is airline passenger reservation data. Consider what a terrorist must do to successfully bring off an attack. He must be trained; he must receive funding; he must meet with his handlers to receive direction; he must enter the country he means to strike; and he must case his intended targets. Each of those steps typically involves travel. That’s why the 9/11 Commission emphasized that, for terrorists, the ability to travel is “as important as weapons.”⁷ And it called on the government to deploy “[i]nformation systems able to . . . detect potential terrorist indicators . . . at consulates, at primary border inspection lines, in immigration services offices, and in intelligence and enforcement units.”⁸

Al Qaeda is dependent upon travel, and each time an operative boards a plane or crosses an international border, we have an opportunity to detect and capture him. Doing so requires that officials have access to information about airline passengers. In the trade, this data is known as “PNR,” or Passenger Name Records. PNR consists of basic personal information that travelers provide to airlines or travel agents in the course of booking airline reservations. PNR is hardly a dossier of passengers’ most intimate secrets. It typically includes pedestrian data such as name, passport number, frequent flyer number, address, telephone number, and so on. Airlines that fly to and from the United States are required by law to provide DHS this information (more on this requirement below). DHS then uses a computerized system – the Automated Targeting System,

⁴ Homeland Security Act of 2002, § 202, Pub. L. No. 107-296, 116 Stat. 2135, 2149-50 (2002).

⁵ Intelligence Reform and Terrorism Prevention Act of 2004, § 1016, Pub. L. No. 108-458, 118 Stat. 3638, 3664-70 (2004).

⁶ Cf. RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 209 (2006) (arguing that “[i]ntelligence is cheap relative to defensive measures such as hardening potential targets, sealing the nation’s borders, and inspecting cargoes,” but cautioning that “[i]ts cheapness is seductive, fostering the illusion that intelligence can be perfected at modest cost”).

⁷ NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 384 (2004).

⁸ *Id.* at 385.

or “ATS” – to analyze the data to help determine which of the 87 million passengers who enter the United States by air each year should be subject to a little extra scrutiny.⁹

The information contained in PNR may be fairly simple, but it is a powerful analytical tool. At the most basic level, collecting PNR and passenger manifest data enables officials to check travelers’ names against watchlists of known or suspected terrorists.¹⁰ (It also enables the government to resolve potential false positives more expeditiously. Suppose one “M. Atta” – a name that also appears on the no fly list – is traveling from London to JFK. If the only thing officials know about the passenger is his name, he likely is going to be pulled aside at Heathrow and asked a number of questions to establish his true identity. Making more information available to the government allows that process of identity resolution to take place behind the scenes, and more quickly. If officials have not just M. Atta’s name, but also his date of birth, his passport number, his fingerprints, and so on, it becomes possible to know immediately whether this is a man to worry about, or whether he’s an innocent with the misfortune of sharing a name with an international terrorist. PNR thus is more than just a useful counterterrorism tool. It also has the potential to produce meaningful customer service benefits for individual travelers.)

More sophisticated analytics are possible as well. By using simple forms of link analysis, PNR makes it possible to discover hidden connections between known terrorists and their unknown associates. If a traveler has used the same phone number or mailing address as Khalid Shaikh Mohammed, mastermind of the September 11 plot, he probably merits a closer look than a typical airline passenger.

Let’s dwell on that point for a moment. According to a Markle Foundation report, if counterterrorism investigators had been able before 9/11 to apply rudimentary link analysis techniques to airline reservation data and related information, they could have uncovered the ties among all 19 of the hijackers.

Start with two men who helped fly American Airlines flight 77 into the Pentagon: Nawaq Alhamzi and Khalid Al-Midhar. Their names appeared on a U.S. watchlist, because they previously had been spotted at a terrorist meeting in Malaysia. So they would have been flagged when they bought their tickets. Tugging on that thread would have revealed three other hijackers who used the same addresses as the first two: Salem Al-Hamzi, Marwan Al-Shehhi, and Mohamed Atta, the plot’s operational ringleader. Officials would have discovered another hijacker (Majed Moqed) who used the same frequent-flyer number as Al-Midhar. Five other hijackers used the same phone numbers as Mohamed Atta: Fayez Ahmed, Mohand Alshehri, Wail Alshehri, Waleed Alshehri, and Abdulaziz Alomari. That’s eleven of 19. Officials could have found a twelfth hijacker in an INS watch list for expired visas (Ahmed Alghamdi), and the remaining seven could have been flagged through him by matching other basic information.¹¹

⁹ See U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43,650, 43,651 (Aug. 6, 2007).

¹⁰ See *id.*.

¹¹ PROTECTING AMERICA’S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 28 (2002). One of the authors was a member of that task force.

PNR is good for more than for Monday morning quarterbacking; it has produced a number of tangible successes. For instance, in 2006, at Minneapolis-St. Paul airport, DHS officials used PNR data and other information to flag a high-risk traveler for additional scrutiny before he arrived. Once the passenger was referred to secondary inspection, it was discovered that he had a manual on how to make Improvised Explosive Devices, or “IEDs” – the kind of bombs terrorists use to kill and maim American forces in Iraq and Afghanistan. Inspecting the traveler’s computer, officers also found video clips of IEDs being used to kill soldiers and destroy vehicles, as well as a video on martyrdom. The passenger later pled guilty to visa fraud.¹²

II. PNR and the Law of Data Privacy

The legal authorities – constitutional, statutory, and international – under which the United States collects and uses these sorts of information are fairly straightforward. Let’s start with the Constitution. Every first-year law student can recite that the Fourth Amendment’s prohibition on unreasonable searches and seizures generally requires the government to obtain a search warrant before gaining access to facilities or information in which the holder has a “reasonable expectation of privacy.”¹³ Over the course of several decades, the Supreme Court has held that a person generally has no such reasonable expectation in data he voluntarily turns over to a third party in the ordinary course of business.

For example, the government need not obtain a search warrant before installing a pen register or trap and trace device – which collect data about the numbers dialed or received by a particular telephone, but not the content of the conversations themselves – because the caller necessarily reveals that information to the phone company when he places a call.¹⁴ Nor is a warrant needed when the government asks a bank to turn over a customer’s financial records. Because a “depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government,” a depositor has no “legitimate ‘expectation of privacy’ in . . . information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”¹⁵

The “third party doctrine,” as it is known, has come in for its fair share of criticism. Maybe more than its fair share. Orin Kerr has dubbed it “the *Lochner* of search and seizure

¹² See Remarks of Stewart Baker, Assistant Sec’y for Policy, Dep’t of Homeland Security, at the Ctr. for Strategic and Int’l Studies (Dec. 19, 2006), http://www.dhs.gov/xnews/speeches/sp_1166557969765.shtm.

¹³ *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

¹⁴ See *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.”).

¹⁵ *United States v. Miller*, 425 U.S. 435, 442, 443 (1976); see also *id.* at 443 (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

law.”¹⁶ The leading criminal law treatise pronounces it “dead wrong,”¹⁷ and other scholars aren’t much more temperate in their denunciations.¹⁸ More recently, Professor Kerr has mounted a defense of the doctrine, arguing that it is sound because it ensures technological neutrality. Under the third party doctrine, the same amount of privacy protection is available regardless of whether a criminal personally ventures into public spaces to commit his crimes, or remains in the private sphere by commissioning a third party to assist the criminal enterprise.¹⁹

Whatever the strengths or weaknesses of the third party doctrine, PNR is a fairly straightforward application of it. As is true with phone numbers and financial information, travelers voluntarily provide basic personal data to airlines or travel agents in the ordinary course of booking a reservation – the name they wish to appear on the ticket, the method of payment, a phone number at which they can be contacted in the event there is a schedule change, and so on. Again, like phone numbers and financial data, providing this information to an airline doesn’t simply help facilitate the transaction. The transaction wouldn’t be possible without it. DHS’s use of PNR thus fits pretty comfortably within established constitutional norms concerning government access to data voluntarily conveyed to third parties.

Even those who don’t share the Supreme Court’s gloss on the Fourth Amendment – that a person *never* has a reasonable expectation of privacy in data turned over to third parties, no matter how sensitive it is or how narrowly he intends it to be distributed, because he assumes the risk it will find its way into the government’s hands – should be able to conclude that PNR works no undue harm to travelers’ privacy interests. A narrower principle is available here. A depositor typically shares data with his bank in the expectation that the bank, as his agent, will protect it from further disclosures to outside entities. By contrast, a passenger may well benefit if airlines or travel agents provide his PNR data to the government. Doing so can lead to a better customer service experience at the border. In the absence of PNR, U.S. Customs and Border Protection officials would need to ask arriving passengers several dozen questions at the passport control booth, backing lines up to the tarmac in the process. Providing that information electronically in advance of arrival allows the vast majority of passengers to enter the country quickly as the government focuses its scarce resources on the travelers most likely to pose a threat. Passengers don’t merely “assume the risk” that airlines will share their reservation data with the government. It is in their interest that airlines do so.

The statutory framework surrounding PNR is equally straightforward. Less than two months after the September 11 terrorist attacks, Congress enacted the Aviation and Transportation Security Act of 2001. Section 115 of that legislation directs all air carriers that fly to the United States to provide the government with a passenger and crew manifest (including

¹⁶ Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (citing *Lochner v. New York*, 198 U.S. 45 (1905)).

¹⁷ 1 WAYNE R. LAFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 2.7 (4th ed. 2004).

¹⁸ *See, e.g.*, Clark D. Cunningham, *A Linguistic Analysis of the Meanings of “Search” in the Fourth Amendment: A Search For Common Sense*, 73 IOWA L. REV. 541, 580 (1988) (indicating that the Supreme Court’s third party decisions “top the chart of the most-criticized Fourth Amendment cases”).

¹⁹ *See* Kerr, *supra* note 16, at 564-65.

each passenger and crew member’s full name, their dates of birth, their passport numbers, and “[s]uch other information” as is deemed “reasonably necessary to ensure aviation safety”), as well as “passenger name record information.”²⁰

International law likewise recognizes the legitimacy of American efforts to collect reservation data. The 1944 Chicago Convention on International Civil Aviation acknowledges that every nation has “complete and exclusive sovereignty” over its airspace.²¹ As a corollary, Article 11 of the agreement expressly directs airlines to comply with a country’s laws “relating to the admission to or departure from its territory of aircraft engaged in international air navigation.”²² A similar obligation attaches to individual passengers. Article 13 requires passengers – and those who act on their behalf, such as airlines – to comply with a country’s laws governing “the admission to or departure from its territory,” including “regulations relating to entry, clearance, immigration, passports, customs, and quarantine.”²³

As we’ve seen, one of the laws “relating to . . . admission . . . or departure” with which U.S.-bound airlines must comply is the obligation that they share PNR and other passenger information. The U.S. then uses that data for the various purposes spelled out in the Convention – e.g., deciding whether a particular traveler should be allowed to enter the country, assessing his immigration status, checking the authenticity of his passport, and so on. Indeed, the Convention expressly requires airlines to collect and turn over basic information about the passengers they carry. When it was signed in 1944, data-collection and –processing capabilities were still in their infancy. Yet the Convention still obliges “[e]very aircraft” that flies internationally to carry “a list of [passengers’] names and places of embarkation and destination,”²⁴ and to make that list available to authorities upon arrival.²⁵ That’s an embryonic form of PNR.

Not only is collection and analysis of PNR data legally permissible under the Chicago Convention, the agreement actually encourages it as sound public policy. States have an obligation under the Convention “to prevent unnecessary delays” to passengers, “especially in the administration of the laws relating to immigration, quarantine, customs, and clearance.”²⁶ PNR helps accomplish exactly that. Advance transmission of reservation data enables the U.S. to begin screening passengers while their flights are still in the air, or even before they depart. That means officials are able to wave the vast majority of arriving passengers through immigration and customs with very little additional face-to-face scrutiny. PNR lets officers speed these bona fide travelers along while focusing their attention on the small number of passengers who present special risks.

III. The EU Strikes Back

²⁰ 49 U.S.C. § 44909(c)(2), (3).

²¹ Chicago Convention on International Civil Aviation art.1, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

²² *Id.* art. 11.

²³ *Id.* art. 13.

²⁴ *Id.* art. 29.

²⁵ *Id.* art. 16.

²⁶ *Id.* art. 22.

Europe's approach to data privacy is different from that of the United States. While U.S. courts generally hold that sharing data with a third party vitiates one's expectation of privacy, EU law provides that government access to information typically must be on the basis of the data subject's "consent." The EU's Charter of Fundamental Rights sweepingly proclaims that "[e]veryone has the right to the protection of personal data concerning him or her"; it further provides that "[s]uch 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."²⁷ To European eyes, the American approach to data privacy must look incomplete, if not downright primitive.

To say that Europe's privacy values are "different" than America's is not to say that they are somehow "better" or "more protective." Americans and Europeans simply have different understandings of what is meant by privacy, to say nothing of different views on how to go about protecting it. As one scholar has observed:

[W]e will not do justice to our transatlantic conflicts if we begin by declaring that American privacy law has "failed" while European privacy law has "succeeded." That is hogwash. What we must acknowledge, instead, is that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy.²⁸

In a nutshell, European privacy law aims primarily at protecting human dignity against the depredations of mass media, while the American law of privacy is generally preoccupied with preserving individual liberty against government encroachments.²⁹ Perhaps equally divisive, Americans and Europeans have different legal styles even when they seek to protect the same basic interest. European privacy law soars with generalities; American privacy law is relentlessly particular.

As a result, American privacy law looks partial and niggling from a European standpoint. But from America's vantage point, European privacy law often looks long on talk and short on results. Take wiretapping. In the United States, protections against electronic surveillance are more a matter of procedure than grand theory. Police cannot tap a suspect's phone unless they obtain a "superwarrant"³⁰ – in addition to establishing probable cause, they must also exhaust other means of obtaining the information and take steps to minimize the interception of other conversations.³¹ In Europe, the procedures are looser, with predictable results. French and

²⁷ Charter of Fundamental Rights of the European Union art. 8(1), (2), Dec. 7, 2000 O.J. (C 364) 10.

²⁸ James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151, 1160 (2004).

²⁹ *See id.* at 1219.

³⁰ Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT ACT: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620 (2003).

³¹ *See* 18 U.S.C. § 2518(3)(c), (5).

German phones are tapped ten to 30 times more frequently than their American counterparts, and the rates in Italy and the Netherlands are an order of magnitude greater still – between 130 and 150 times the American rate.³²

Preventive detention presents similar differences. Criminal suspects in the United States typically are brought before a judge for arraignment – the formal filing of charges – within 48 hours of being arrested.³³ Yet the European Convention of Human Rights acknowledges the power of member states to subject a person to preventive detention “when it is reasonably considered necessary to prevent his committing an offense.”³⁴ In France, it’s even possible to be kept in preventive detention after completing one’s sentence, if authorities consider the person dangerous or a likely recidivist.³⁵

Nor are the differences limited to criminal procedure. Most European countries require their citizens to carry an official identity card and to display it on demand. Americans have never accepted such a requirement, and most would consider it a violation of their privacy. Some European nations even have the authority to veto the names parents have picked for their newborns, and the European Court of Human Rights has held that such veto power does not violate personal privacy.³⁶ That sort of government interference would be anathema to Americans, whose Constitution protects the privacy-based right to direct the upbringing of one’s children.³⁷

What’s noteworthy is not just that America and Europe understand personal privacy in different terms, or pursue that mutual goal through different means. These sorts of disagreements are inevitable, even among countries that spring from a common political culture. What’s noteworthy is the newfound willingness of some in Europe to assume that values differing from European values, and even procedures differing from European procedures, are presumptively inadequate.

In May 2004, the Department of Homeland Security signed an agreement with representatives of the European Union governing the transmission of PNR for flights originating in Europe. A principal impetus for the agreement was the fear of some European airlines that complying with their obligation under U.S. law to provide PNR would run afoul of European data privacy law. The airlines thus faced a Hobson’s choice: Either provide PNR and risk liability in Europe, or refuse to provide PNR and risk liability in the United States. The 2004 agreement was designed to alleviate those concerns.

³² See Whitman, *supra* note 28, at 1159 & n.40.

³³ Cf. *County of Riverside v. McLaughlin*, 500 U.S. 44, 55-58 (1991).

³⁴ Convention for the Protection of Human Rights and Fundamental Freedoms, Dec. 10, 1948, art. 5(1)(c), Europ. T.S. No. 5.

³⁵ Press Release, Amnesty International, *France: Amnesty International’s Concerns on “Preventive Detention” Bill* (Feb. 8, 2008), <http://www.amnestyusa.org/document.php?lang=e&id=ENGEUR210022008>.

³⁶ See Whitman, *supra* note 28, at 1216-17 & n.327 (citing *Guillot v. France*, App. No. 22500/93 (Eur. Ct. H.R. Oct. 24, 1006)).

³⁷ See, e.g., *Pierce v. Society of Sisters*, 268 U.S. 510, 534-35 (1925); *Meyer v. Nebraska*, 262 U.S. 390, 399 (1923).

Though well intentioned, the agreement sharply limited DHS's ability to collect, use, and share PNR data. Under its terms, DHS was only allowed to use European PNR in certain kinds of investigations – namely, cases involving “terrorism” or “serious crimes . . . that are transnational in nature.”³⁸ That meant PNR was off the table in domestic criminal cases – even serious ones, such as investigations of kidnapping and child exploitation. DHS further was barred from collecting certain types of passenger data, such as frequent flyer numbers.³⁹ (Recall that comparing passengers' frequent flyer numbers before 9/11 would have enabled investigators to identify Majed Moqed, one of the hijackers on American flight 77.⁴⁰) The agreement also called on representatives of the EU to engage in periodic “adequacy” audits of DHS's use of PNR⁴¹ – i.e., to assess whether the United States was satisfying European data privacy standards.

Most significant of all were the restrictions on DHS's ability to share information. Not only was DHS barred from routinely sharing European PNR with outside entities like the FBI or state and local law enforcement; it was even barred from doing so within DHS. U.S. Customs and Border Protection – the DHS component with immediate custody of PNR data – was allowed to use it, but other DHS entities could only gain access on a case-by-case basis.⁴² In effect, the European Union had rebuilt the “wall” between intelligence and law enforcement, a wall that Congress quite consciously tore down after September 11.

The EU also sought to insert European privacy norms into the United States' relationships with other countries. In the run-up to the 2007 Cricket World Cup, DHS entered a data sharing arrangement with a number of the Caribbean countries set to host the games. These nations agreed to share passenger information with DHS, and DHS in turn would analyze it to determine whether any high-risk persons were traveling to those countries.⁴³ When the EU learned of the arrangement, it threatened to impose trade sanctions on the participating Caribbean nations. The Caribbean countries thus found themselves caught in the crossfire of a policy dispute between Brussels and Washington, much like the European airlines whose liability fears initially spawned the 2004 PNR agreement.

The 2004 agreement wasn't just inconsistent with American law and policy; it was in tension with international law. The Chicago Convention repeatedly stresses the importance of equal treatment: Aircraft, crew, and passengers may not be subjected to special burdens – or extended special benefits – based on their country of origin. Thus the Convention requires states

³⁸ 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 (July 9, 2004) [“2004 PNR Agreement”].

³⁹ *Id.* at 41,547.

⁴⁰ *See supra* note 11 and accompanying text.

⁴¹ 2004 PNR Agreement, 69 Fed. Reg. at 41,547.

⁴² *Id.* at 41,545.

⁴³ *See* U.S. Dep't of Homeland Security, Office of Inspector General, Management of Dep't of Homeland Security Int'l Activities and Interests 39 (June 24, 2008), http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_08-71_Jun08.pdf.

to apply their laws “to the aircraft of all contracting States without distinction as to nationality.”⁴⁴ It obliges nations to make available airport facilities, such as radio services, “under uniform conditions to the aircraft of all the other contracting States.”⁴⁵ And it allows states to bar planes from carrying hazardous cargo, but only if “no distinction is made in this respect between its national aircraft . . . and the aircraft of the other States.”⁴⁶ In short, the Chicago Convention aims at uniformity. Yet the EU was seeking to carve out special rules for European PNR. Brussels effectively was arguing that, notwithstanding the fact that Australian and Japanese – and American – carriers had to comply with U.S. law, European airlines should receive special treatment.

The European Parliament wasn’t fond of the 2004 agreement either, though for different reasons. In a lawsuit before the European Court of Justice (ECJ), the parliamentarians claimed both that the agreement’s terms were inconsistent with EU privacy law, and that the EU lacked legal authority to enter into it. On May 30, 2006, the ECJ handed down its decision.⁴⁷ The court sidestepped the Parliament’s privacy-based claims, and struck down the agreement as beyond the EU’s powers.

A little background is needed to make sense of that ruling. Originally, the European Union was created for economic reasons – to harmonize and reduce trade barriers and create a free-trade area. Matters relating to trade and travel (known as “First Pillar” issues) are ones where the sovereign member states ceded substantial powers to the new central government in Brussels. At the same time, the member states retained most of their traditional powers in matters of foreign policy and national defense (“Second Pillar” issues), as well as law enforcement and internal security (“Third Pillar” issues). At the risk of oversimplifying, it might be helpful to think of the architecture of Europe’s legal system as resembling nineteenth century American federalism. Brussels is the seat of a strong but limited central government that wields a defined set of powers, while the residual powers not granted to Brussels are retained by the separate member states.

As the court pointed out, the EU adopted the PNR agreement under its First Pillar powers – the ones governing trade, travel, and other economic issues related to the common market. But even though air carriers collect PNR data for commercial purposes, the U.S. law requiring transfer of the data and the agreement limiting the U.S. government’s use of that data were not directed at trade regulation. The purpose of the law was to assist in detecting potential terrorists and criminals. According to the court, the agreement “concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.”⁴⁸ As a result, the EU had no power under its First Pillar authorities to sign the agreement. If the EU wanted a PNR agreement, it would have to

⁴⁴ Chicago Convention on International Civil Aviation art.11, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

⁴⁵ *Id.* art. 15.

⁴⁶ *Id.* art. 35.

⁴⁷ *See* Joined Cases C-317/04 & C-318/04, *European Parliament v. Council of the European Union & Commission of the European Communities*, 2006 E.C.R. I-4721.

⁴⁸ *Id.* ¶ 57.

enter it under the Third Pillar. Again, at the risk of oversimplifying, it's as if the United States Supreme Court held that Congress lacked power under section 5 of the Fourteenth Amendment to ban private commercial establishments from engaging in racial discrimination,⁴⁹ but reasoned that it could enact the same prohibition under the Commerce Clause.⁵⁰

The denouement came in 2007. After signing an interim agreement in October 2006,⁵¹ DHS and the European Union reached a final agreement in July of the following year. The 2007 edition departs from its 2004 predecessor in a number of important respects. The new agreement retains the original use limitation – “terrorism” and “serious crimes . . . which are transnational in nature” – but it now emphasizes that PNR can be used for any other purpose if “otherwise required by law.”⁵² The 2007 agreement reduces the number of data elements from 35 to 19, mainly by combining the old elements into new categories, but it also makes clear that certain types of information that previously were off limits can now be collected, including frequent flyer data.⁵³

In the 2007 agreement, the EU once again deems that DHS ensures an “adequate” level of data protection.⁵⁴ But this time important reciprocity provisions have been added, which clarify that the EU is no longer sitting in judgment of American policy choices. Instead of a one-way “adequacy” audit, the agreement contemplates that DHS and EU representatives will jointly participate in assessments “with a view to mutually assuring the effective operation and privacy protection of their systems.”⁵⁵ The agreement also states that neither DHS nor the EU will ask the other to implement data protection measures that are more stringent than the ones it is willing to adopt itself.⁵⁶ And the EU pledged that, as a “[c]oncomitant[]” of its conclusion that DHS’s data practices are “adequate,” it “will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds.”⁵⁷ That clause will help ensure that other countries don’t get caught in any future transatlantic crossfire.

The information sharing terms represent the most significant departure from the 2004 agreement. The signatory of the agreement is DHS as a whole, not a subsidiary DHS

⁴⁹ See *The Civil Rights Cases*, 109 U.S. 3 (1883).

⁵⁰ See *Heart of Atlanta Motel v. United States*, 379 U.S. 241 (1964).

⁵¹ See *Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record Data*, 72 Fed. Reg. 348 (Jan. 4, 2007).

⁵² Letter from Michael Chertoff, Secretary, U.S. Dep’t of Homeland Security, to Luis Amado, President, Council of the European Union at 1 (July 26, 2007) [“Chertoff letter”], <http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usltrtoeu.pdf>.

⁵³ See *id.* at 2.

⁵⁴ Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) ¶ 6, July 26, 2007, <http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf>.

⁵⁵ *Id.* ¶ 4.

⁵⁶ *Id.* ¶ 5.

⁵⁷ *Id.* ¶ 6.

component. That means PNR information can be shared within DHS without restriction – provided, of course, that it is used for purposes of combating terrorism or serious transnational crimes. Likewise, the 2007 agreement expressly contemplates that DHS may share PNR with “other domestic government authorities.”⁵⁸ The new agreement thus implements Congress’s instructions to eliminate barriers to effective information sharing.

The PNR story has a happy ending – Washington and Brussels signed an agreement with which both sides were satisfied – but the trend it represents is still troubling. DHS’s passenger screening system was deployed at the direction of Congress and in reliance upon on a series of Supreme Court rulings; in effect, all three branches of the federal government participated in the decision. The EU could have acknowledged that, while American law policy did not comport with its own preferences, the United States nevertheless was entitled as a sovereign to choose differently. It did not. Instead, Brussels claimed the right to sit in judgment of American data privacy practices.

The European Union’s tactics throughout the PNR episode posed fundamental challenges to basic principles of multilateralism and international law. The EU never explained why its internal commercial data protection law should be read in a fashion so at odds with the multilateral Chicago Convention. It never justified its assumption that no law governing data used in criminal investigations could be adequate unless it was nearly identical to European law. Nor did the EU clarify why European data-privacy rules should trump American data-disclosure requirements. It would have been hard-pressed to do so. The Restatement (Third) of Foreign Relations Law actually reflects the opposite principle: Legal requirements “by the state in whose territory the act is to be carried out ordinarily prevail over orders of other states.”⁵⁹ When a private party is subject to conflicting laws of two nations, it generally must comply with the laws of the country where the conduct in question occurs, not the country of which it is a national. Under the Restatement, U.S. laws directing airlines to turn over PNR were entitled to priority. Finally, and most troubling for large multinational enterprises, the European Union seemed almost enthusiastic about threatening airlines with sanctions as a way of attacking American policies and practices with which it disagreed. For obvious reasons, putting private actors in a position of having to violate the laws of one sovereign in order to heed the laws of another is dubious practice under international law. One of the key goals of the Restatement is “to protect persons caught between conflicting demands.”⁶⁰

Regrettably, threats against private firms are a growth industry on the Continent. The European Union seems to have concluded that the tactic should be applied to new fields, including financial records. After 9/11, the U.S. Treasury Department served subpoenas on the Belgium-based Society for Worldwide Interbank Financial Telecommunication, or SWIFT, a financial data exchange that monitors banking transactions across the globe. Treasury wanted access to bank records that could be used to identify and locate al Qaeda financiers, and SWIFT

⁵⁸ Chertoff letter, *supra* note 52, at 1-2.

⁵⁹ RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 441 cmt. b (1987).

⁶⁰ *Id.* § 441 cmt. a.

complied with the subpoenas.⁶¹ After EU officials called for a criminal investigation, Belgian authorities declared that the consortium had violated European data protection law:

SWIFT should have, as of the beginning, been aware of and should have taken into account the fact that, in addition to the application of U.S. law, the fundamental rules of European law on data protection had to be complied with, in particular the proportionality principle, the limitation of the retention of data for the period required by processing requirements, the transparency principle, the requirement of an independent control and the existence – prior to any transfer outside the European Union – of standards ensuring an adequate level of protection in the country of destination.⁶²

What is significant about these requirements is that SWIFT could not meet any of them. In essence, the authorities were saying that, before complying with U.S. law, SWIFT had an obligation to ensure that the U.S. government met European procedural and substantive legal standards. Since no private actor has the leverage to demand such assurances, particularly after receiving a subpoena, such a requirement dooms the actor to simply deciding which law to violate.

The U.S. responded to the EU's tactics by suggesting that threats against private firms should be out of bounds in transatlantic privacy disputes. Reasoning that U.S. and European criminal data protection standards were not far apart in practice, the U.S. proposed that a "High Level Contact Group" try to reconcile U.S. and European norms with a view to declaring them broadly consistent so that private companies could continue to obey the investigative demands of both jurisdictions without fear of liability. This effort is ongoing. As expected, broad agreement has been reached on criminal data protection principles, but thus far the European Union has been reluctant to adopt a straightforward assurance that private companies will not be put in a position of uncertainty about their data protection liability when they comply with subpoenas and other investigative requirements. This assurance is precisely what private firms receive when a jurisdiction is declared "adequate" under European data protection law, and the talks have been stalled by the High Level Contact Group's failure to provide an equivalent assurance even after reaching broad agreement on data protection standards. Nonetheless, progress continues to be made, and an agreement that provides assurances to multinational companies (and criminal investigators) seems within reach at this writing.

IV. Explanations, Implications, and Solutions

What accounts for Brussels's apparent determination to export its data privacy values throughout the globe, and its insistence that other countries adhere to European norms? Why would Europe sacrifice its traditional commitment to multilateralism and international law in

⁶¹ See Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

⁶² Commission for the Protection of Privacy, Control and Recommendation Procedure Initiated with Respect to the Company SWIFT (Dec. 9, 2008) (Belgium), http://www.privacycommission.be/en/static/pdf/cbpl-documents/a10268302-v1-0-151208_translation_recommswift_fina.pdf.

order to restrict terrorism investigations in other countries? A number of possible explanations come to mind, some more creditable than others.

Part of it is good faith substantive disagreement about the meaning of privacy and how best to preserve it. To Continental eyes, the American approach to data privacy looks narrow and lacking in broad protective principles. Indeed, the EU may not even recognize its actions as intrusive-, seeing them rather as beneficent efforts to nudge their American cousins toward right thinking. Another explanation is the occasionally stated desire of some European policymakers that the EU serve as a counterweight to the American “hyperpower.” By binding the United States in a web of international obligations, as the Lilliputians bound Gulliver, the EU is able to project its own power.⁶³

Neither of those observations is especially original. A third, and less noticed, possible reason for Brussels’s privacy evangelism has to do with the distribution of powers within Europe. Recall that the EU’s central government has broad authority when it comes to trade, travel, and other First Pillar economic powers, but the individual member states remain sovereign over issues such as national defense and internal security. It’s not surprising that Brussels would want to accumulate new powers traditionally held by the member states, especially the national security powers that have assumed even greater importance in the post-9/11 era.

The question is how to do so. A shrewd way for Brussels to expand its power is to take familiar and uncontroversial First Pillar rules that originally were crafted for commercial purposes and relocate them into new law enforcement and counterterrorism contexts. The central government gains new authorities, since it is transplanting broad authorities into realms where its power is nominally more limited, and it does so in a way that is less likely than a naked power grab to attract the attention of the member states that stand to lose from the arrangement. That may be what happened in 2004, when the EU sought to apply commercial data privacy norms to what was at root a law enforcement and counterterrorism matter. The ECJ later struck down the 2004 PNR agreement as *ultra vires*, but by then a political consensus had congealed in Brussels that negotiations on PNR were necessary and that only the EU could conduct them.

In general, transatlantic conflict has proven a reliable way for Brussels to expand its authority. Sometimes the EU accumulates new powers, not by *sotto voce* transplantation of established First Pillar rules, but by persuading its member states to grant it an express mandate to negotiate on their behalf with a foreign interlocutor. Because member states have “a duty of loyal cooperation” with the European Union, they may not undercut Brussels’ negotiators by adopting rules inconsistent from those being negotiated for the EU as a whole. But this apparently straightforward principle means that, simply by opening negotiations with the U.S., Brussels gains a veto over new areas of member state action.

Once an agreement is reached, the expansion of authority becomes even more explicit. Under EU law, if a foreign country signs an agreement with Brussels concerning a Second or Third Pillar matter, and the EU’s member states approve the agreement, then Brussels will have

⁶³ See, e.g., Robert Kagan, *Power and Weakness*, POLICY REV. (June & July 2002).

new legal authority over the member states' practices as long as it couches its role in terms of enforcing the agreement. This is *Missouri v. Holland*⁶⁴ on steroids. In that case, Justice Oliver Wendell Holmes held that Congress had power to regulate lands used by migratory birds as necessary and proper to a treaty with Canada, even though it lacked power to adopt the same requirements under the Commerce Clause. In effect, Congress can acquire new legislative powers simply by ratifying a treaty. The EU's powers would make Justice Holmes envious: Brussels can bootstrap its way into new authorities not only by ratifying a treaty, but by entering a less formal international agreement.

The result is not surprising. Bureaucratic entrepreneurs in Brussels who want to maximize their authority find that transatlantic conflict, transatlantic negotiations, and transatlantic agreements all contribute to that cause. In short, a European Union that hopes to accumulate new powers will want to find new international disagreements and enter into new international agreements. (The dynamic we have described – the creation of conflict and its resolution as a way to expand turf – will change if and when the proposed European constitution is ratified. If member states decide to grant broad new powers to Brussels, the EU won't have the same need to create and resolve disputes in order to gain jurisdiction, because the new constitution will have accomplished that already. Voters in France and the Netherlands rejected the constitution in 2005; those referenda effectively killed it, since all 27 EU members must ratify an agreement for it to go into effect. More recently, the so-called "Lisbon treaty" has resurrected most of the constitution's substantive features. Irish voters said no to Lisbon in 2008; as of this writing the ratification process is ongoing.⁶⁵)

American policymakers should be aware of this dynamic when they consider entering into international negotiations or agreements with the European Union and the European Commission. Simply launching such negotiations may tilt the balance of authority between individual member states and Brussels. For that reason, policymakers should always ask themselves whether agreements with individual member states would be preferable, and whether an EU-wide agreement will create incentives to provoke conflicts in the future. We expect that amicable agreements on topics of mutual U.S.-EU interest will raise these concerns only rarely, if ever. But the United States should be especially wary of signing agreements when the issue is one on which Washington and Brussels have widely divergent policy preferences, or incident to a prolonged or contentious dispute with the EU. In those circumstances, the U.S. may be better served by working with individual countries.

That bridge has been crossed, of course, in the context of data protection and antiterrorism measures. The U.S. and the EU have already negotiated several arrangements in this field. What remains is to clean up the mess left by the talks. The U.S. and EU should revitalize the High Level Contact Group and develop a shared framework of principles by which future transatlantic disputes over criminal data protection will be resolved. Agreement is within reach on at least the broad principles of how to protect privacy while implementing effective antiterrorism measures. The two jurisdictions should also acknowledge that this broad

⁶⁴ 252 U.S. 416 (1920).

⁶⁵ See Stephen Castle & Judy Dempsey, *Europe Pushes Ireland to Help Save Treaty*, N.Y. TIMES, June 20, 2008, at A11.

agreement revolves around a few principles that should inform future international data protection arrangements⁶⁶:

- Modesty. It's inevitable that the U.S. and its allies in Europe will adopt different solutions to commonly recognized problems. It's also inevitable that they will disagree on what amounts to a problem at all. When such disputes arise, both Washington and Brussels should show a measure of restraint. Each should acknowledge that it does not have a monopoly on sound policy ideas, and that its partner is entitled to chart a different course than the one it prefers. Nowhere is modesty more necessary than in disputes related to privacy policy. America and Europe take different roads to the protection of individual rights, and in some cases they may understand privacy differently, but neither side should forcibly convert the other to its own way of thinking.
- Reciprocity. Neither the United States nor the European Union should demand that the other take actions that it is not prepared to take on its own. This is of course an elementary principle of international relations, but it bears reemphasizing. The reciprocity principle makes sense from the standpoint of fairness. It also is valuable to the extent it can help prevent conflict among allies. Reciprocity can discourage either partner from proposing arrangements that are likely to prove so controversial as to disrupt the relationship. (Care must be taken, however, to ensure that legitimate reciprocity concerns do not blossom into restraints on creativity and innovation.)
- Private business. Private firms whose activities are intertwined with national security operations – airlines, banks, and others – should not be used as pawns in disputes between Washington and Brussels. When the U.S. and EU disagree about how a particular controversy should be resolved, private businesses may well find themselves subject to conflicting legal requirements. The two partners should agree that they will not threaten to impose civil liability or other penalties on companies as a way of strengthening their respective hands in intergovernmental negotiations.
- Third countries. A similar principle should apply to relationships with third countries. Washington often will seek to enter into arrangements with independent nations that Brussels finds objectionable, and vice versa. The U.S. and EU should commit to not interfering in each other's independent relationships with third countries – for example, by threatening to retaliate against nations that agree to undertake cooperative initiatives with the other.

* * *

Even the best of friends sometimes have disagreements. The United States and the nations of Europe remain strategic partners on virtually every major issue of the day, from trade and commerce to foreign affairs – and, crucially, in the struggle against global terrorism. Yet, at the margins, the two sides inevitably will have different policy preferences, and those divergent priorities just as inevitably will produce transatlantic conflict. When disputes arise, as they did

⁶⁶ These principles echo the recommendations of a task force chaired by the Center for Strategic and International Studies and The Heritage Foundation. See *HOMELAND SECURITY 3.0: BUILDING A NATIONAL ENTERPRISE TO KEEP AMERICA SAFE, FREE, AND PROSPEROUS* 12-13 (Sept. 18, 2008). One of the authors was a member of that task force.

with PNR, each partner must be free to chart its own course. The United States should not demand that the Continent adopt American priorities as its own. And the same goes for Europe. Washington is well within its rights to insist that Brussels not interfere with measures the United States believes are needed to protect against terrorist attacks.