

## HSPI Commentary Series

### EUROVISION? LET'S HOPE IT'S FARSIGHTED

HSPI Commentary 19

October 8, 2010

Jayson P. Ahern, Frank J. Cilluffo, and Sharon L. Cardash

As news of an alleged plot to stage a number of coordinated “Mumbai-style” attacks in Europe and possibly the United States continues to unfold, there looms in the background an important but complex matter between the United States and the European Union (EU) that is neither well understood nor resolved: the sharing of Passenger Name Record (PNR) data. What is PNR and why does it matter? The acronym’s eye-glazing quality belies the considerable significance of this tool in the fight against terrorism and serious crime. Yet its continued effectiveness appears to be at risk, perhaps even for the wrong reasons. With terrorist travel a growing concern as increasing numbers of Westerners (including Americans, Australians, Canadians, and perhaps most notably, British and Germans) seek to participate as foreign fighters in jihadi conflict zones—and in some cases, return to their country of residence with intent to do harm<sup>1</sup>—PNR collection and analysis becomes all the more important. Bear with us for a moment as we seek to explain how this instrument has helped saved lives and how we can help ensure that it continues to do so.

PNR data is the information a traveler shares with an airline, such as contact information, method of payment, and itinerary. Collection and analysis of this data for flights into and out of the United States is required by law, and the Department of Homeland Security (DHS) is charged with the task. There have been several US-EU agreements on PNR over time, and the most recent (of 2007) would extend into 2014 unless the European Parliament (EP) votes to do away with it sooner.

Here’s where the facts get tricky. Under the Lisbon Treaty, which entered into force at the close of 2009, the EP became more powerful. Exercising its new authority in the Spring of 2010, the EP initiated a call to replace the US-EU Agreement governing PNR, based in large part upon privacy concerns. While the European Commission (EC), the EU’s executive body, is poised to move forward this Fall on discussions with the EP about how to proceed, renegotiation of the existing

---

<sup>1</sup> Cilluffo, Frank J., Jeffrey B. Cozzens, and Magnus Ranstorp. 2010. “Foreign Fighters: Trends, Trajectories & Conflict Zones.” Washington, DC; Homeland Security Policy Institute  
[http://www.gwumc.edu/hspi/policy/report\\_foreignfighters501.cfm](http://www.gwumc.edu/hspi/policy/report_foreignfighters501.cfm)

agreement remains a possibility as Members of the EP seek to shape both policy and law in this area.

Why should we care? Because PNR data is integral to thwarting terror and serious crime. Remember David Headley, who conspired to aid the 2008 attacks in Mumbai? Caught while trying to travel (to Denmark to assist in a different plot), PNR collection and analysis was critical in identifying him. Or Najibullah Zazi, who conspired in 2009 to attack the New York City subway system? PNR data was used to identify him too, and to disrupt the terrorist network of which he was a part. Notably PNR data on record was used after the fact, as distinct from only in the course of attempted travel. Further, Faisal Shahzad, perpetrator of the fizzled Times Square bombing in May 2010—an attempted act of mass-casualty terrorism for which he was recently sentenced to life in prison—was captured as he attempted to make his escape overseas. Here, PNR in combination with the closely-linked Advanced Passenger Information System (better known as APIS) was important in identifying the suspect, who had managed to escape surveillance and reach the airport.

These best-known cases are just the tip of the iceberg. In 2009 for instance, according to figures in DHS fact sheets available to the public, PNR data together with APIS helped identify “one-third of all known and suspected terrorists ultimately denied entry to the US.” Likewise in 2008, PNR data “enabled DHS to take over 1,800 enforcement actions...ranging from arrests to seizures.” PNR information has also been used to thwart smugglers trafficking in children (by the dozen), and targeting the United States as their destination point. Nor is the significant value of PNR data one-sided. EC documents, too, highlight examples of “PNR analysis yielding information for investigating serious cross-border crime,” including child trafficking, trafficking in human beings, drug trafficking, and credit card fraud.<sup>2</sup>

Against this background, it’s hardly farfetched to suggest that PNR collection and analysis may be expected to continue to prove its mettle—unless, of course, it dries up. The US cannot afford to be blind on this count. Nor can Europe, especially in prevailing circumstances with the system blinking red there. PNR data can help identify terrorists, serious criminals, and people on watch lists, as much as three days before their scheduled travel. Analysis of this data—showing travel patterns evidenced in previous cases, for example—may in turn lead authorities on both sides of the Pond to associates of these known figures, who may themselves be previously unknown to US or EU officials as either terrorists or criminals. As such, and in the hands of trained analysts using it as a decision support tool, PNR is a powerful instrument in our arsenal in the hunt for the worst of the worst. Individuals with minor misdemeanor arrests are not the subject of our argument here.

---

<sup>2</sup> Europa. 2010. “The Passenger Name Record (PNR) - Frequently Asked Questions.” Press Release Dated September 21. Brussels, BE  
<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/431&format=HTML&aged=0&language=EN&guiLanguage=en>

Indeed, it is crucial to understand what PNR collection and analysis is not. First, it is not in itself a panacea, and is instead best understood as being useful in conjunction with other security tools. PNR data is not a substitute for other investigatory means to be pursued by intelligence and law enforcement authorities. At the same time, it has been contended by some that the case of the 2009 Christmas Day failed airline bombing is but one example of PNR data not being used as well as it could have been. While here is not the place for a detailed case-specific treatment, including an assessment of the merits of that claim regarding PNR, the point is that PNR is not, and cannot be, the exclusive be-all and end-all. Second, save in the most exceptional of cases, where life is at risk, DHS will filter out and delete “sensitive information” contained in the PNR. In this context, sensitive information “means data revealing racial or ethnic origin, political opinions, religious or political beliefs,” etc.<sup>3</sup> Privacy is assuredly a critical dimension of any information sharing initiative, and proper safeguards should accompany any such endeavor. To that end, it bears noting that the February 2010 Joint Review of the US-EU PNR Agreement currently in effect (though not conducted by a third party) found no misuse due to DHS collection.

Now is not the time to pull back. To the contrary, a farsighted approach is needed. Only time will tell the role of PNR data, if any, in the ongoing investigation of the latest Euro-plot. But surely it would be shortsighted to undercut an instrument that has consistently proven its considerable worth.

*Jayson P. Ahern is a Principal with the Chertoff Group, LLC, and served as both Acting Commissioner (2009) and Deputy Commissioner (2007-2009), US Customs and Border Protection. Frank J. Cilluffo is Director of The George Washington University Homeland Security Policy Institute (HSPI) and a former Special Assistant to the President for Homeland Security at the White House. Sharon L. Cardash is Associate Director of HSPI.*

*HSPI Commentaries are intended to promote better policy by fostering constructive debate among leading policymakers, academics, and observers. Designed to be timely and relevant, HSPI Commentaries seek to illuminate the issues of the day by raising important questions and challenging underpinning assumptions. Opinions expressed in Commentaries are those of the author(s) alone. Comments should be directed to [hspi@gwu.edu](mailto:hspi@gwu.edu).*

*Founded in 2003, The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan think and do tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.*

---

<sup>3</sup> *Ibid.*