

STATEMENT OF RANKING MEMBER JACKIE SPEIER (D-CA)

Subcommittee on Counterterrorism and Intelligence Committee on Homeland Security

Hearing: “Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel”

October 5, 2011 at 10:00 AM

Thank you for holding today’s hearing on sharing information to combat terrorist travel and the usage of Passenger Name Record (PNR) data.

I would like to welcome our witnesses today and look forward to gaining insights into how the Department of Homeland Security uses PNR, including how DHS protects travelers’ privacy and the future of our international information sharing agreements.

The usage of PNR data is one of the most powerful tools our government has to combat terrorist travel.

When received in a timely fashion, Passenger Name Record data can help flag potential travelers who have no business getting on a plane to the United States, such as people that are on the No-Fly list.

As we know, analyzing PNR can highlight high-risk travel patterns, such as popular routes used by human smugglers and terrorist facilitators; this may be the only way to flag potentially unknown suspects who aren’t on any watchlists, and who on the surface appear like any other traveler.

And PNR can be immensely important in terrorism investigations.

Investigators can use a terror suspect’s past travel history to identify travel to terror safe havens as well as co-travelers who may be associates, which can help to identify and disrupt the entire terror network.

PNR has played a key role in many prominent terror investigations, including that of the 2008 Mumbai attacks plotter David Headley and the attempted Times Square bomber Faisal Shahzad.

But we almost missed Shahzad when he attempted to leave the country; what enhancements to the system have been put in place to address the vulnerabilities exposed by that near-miss?

Effectively combating terror travel hinges on the timely sharing of information, which requires working with the airline companies to get the PNR data quickly and efficiently.

Have these increased demands for timely information placed any undue burdens on the airline companies or to the traveling public?

Equally important to our cooperation with the airlines is our relationship with our foreign partners.

How can we maintain lasting and mutually beneficial agreements with our foreign partners to ensure the timely sharing of PNR data continues?

One such agreement that has been the subject of public scrutiny and some controversy is the one we share with the European Union.

Many European airports serve as the last point of departure to the United States from many high-risk areas of origin, including the Middle East, Africa, and South Asia, so it is of the utmost importance that we maintain the robust sharing of information on travelers flying from Europe to the U.S.

And it is my wish, Mr. Chairman, that the discussion here today does not in any way jeopardize or apply unwanted pressure on the sensitive negotiations that are still ongoing with the European Union.

But we do need to know – how will proposed changes to the agreement affect our screening operations?

Many people, including privacy advocates both here and abroad, have expressed concern about the privacy implications that come with obtaining customers' data from the airlines for counterterrorism purposes.

Although independent reviews of the PNR information sharing program have determined that the usage of PNR data by DHS has never unlawfully violated a traveler's privacy, we must be mindful of these privacy concerns and ensure that DHS continues to uphold stringent privacy restrictions.

The traveling public has the right to a reasonable degree of privacy, and they have a right to be concerned, and I think we need to do a better job of explaining to the public the parameters of the U.S. government's usage of PNR data, why we need it, and how it is applied.

I am eager to learn more about the protections in place – how exactly do we ensure that a traveler's personal information is protected, and how might future modifications to the agreement further impact privacy?

So I hope today that we can positively contribute to that discussion, and clear up some misconceptions about how and why the government uses Passenger Name Records data.

I am also looking forward to learning more about how far DHS has come since 9/11 to effectively analyze data sources such as PNR to identify and mitigate potential threats.

With the systems CBP and DHS has at its disposal now, could we avoid past failures, such as the Christmas Day attack? How important is PNR data to these efforts, and what challenges remain?

I would like to once again thank the distinguished witnesses for appearing before us today, and look forward to working with them to ensure DHS has the tools it needs to combat terrorist travel.