Secretary

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 14, 2007

Dear Member of the European Parliament:

Thank you for the opportunity to appear today before the Committee on Civil Liberties, Justice, and Home Affairs to further our important dialogue on matters critical to the security of the European Union and the United States.

We face a shared challenge in preventing acts of terrorism against our countries and our citizens. At the same time, we share a fundamental and unwavering commitment to protect the civil liberties and privacy that are the hallmarks of all free and democratic nations.

Recent terrorist attacks in Algeria and Morocco, as well as earlier attacks in Madrid and London, the foiled plot this past August against transatlantic aircraft bound for the United States, and the recent convictions of five British terrorists, underscore the serious nature of the threat we face and the importance of developing common tools and approaches to counter this global menace.

One of these tools is Passenger Name Record (PNR) data, which is a limited set of information provided by air passengers traveling between Europe and the United States. PNR data, used in combination with passenger manifest data, allows U.S. officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals so that we can enhance screening of dangerous people and prevent them from boarding commercial aircraft.

Combined with other intelligence, we use PNR data to check for links that might reveal unknown terrorist connections, such as a traveler who has provided contact information overlapping with a known terrorist. It is our ability to identify these hidden links that has made PNR so valuable to our counterterrorism efforts and the reason it is imperative we reach a new understanding regarding how this information will continue to be shared and protected.

Below are several examples of how analyzing PNR data has prevented dangerous individuals from entering the United States.

- In June 2003, using PNR data and other analytics, one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers were not satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints - or at least parts of them - they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq.

- In January 2003, Customs and Border Protection (CBP) officers in Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between

Venezuela and Miami. A corrupt ticket counter agent would identify low-risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami plotted to remove the added bags from circulation prior to inspection by CBP in Miami.

- On March 11, 2005, CBP arrested two individuals for smuggling drugs from London to Chicago. Their PNR information revealed the use of a common credit card. This credit card's reservation history identified a third traveler who had used the same card and listed a second credit card. Analysis of this new credit card number identified three additional travelers. Three of the four new travelers were arrested during subsequent travel for drug smuggling.

- In January 2006, CBP officers used PNR data to identify a passenger posing a high risk for document fraud. The passenger, posing as a citizen of Singapore, was scheduled to depart Korea for the United States. The subject's travel itinerary was targeted by a query using data from recent cases of document fraud in Sri Lanka. CBP officers contacted airline representatives in Korea and requested assistance in verifying the traveler's documents. With airline assistance, CBP determined the subject's travel document was a counterfeit Singapore passport. The subject was in possession of his Sri Lankan passport. The subject was also a positive match to the Transportation Security Administration's No Fly List and suspected of being an armed and dangerous terrorist. The subject was denied boarding for the flight. He was subsequently stopped on another date using the same method of PNR targeting. In the second incident, he attempted to travel to the U.S. using a counterfeit UK passport.

- In February 2006, CBP officers used PNR data to identify a passenger with a high-risk for narcotics possession arriving from the Dominican Republic. The subject, a returning U.S. legal permanent resident, purchased his ticket using cash and made certain changes to his reservation. Upon arrival, the subject was selected for an enforcement exam. During an examination of the subject's personal effects, CBP officers discovered two packages containing heroin. The subject was placed under arrest and turned over to Immigration and Customs Enforcement for prosecution.

- At Boston Logan Airport in April 2006, CBP officers used PNR data to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labeled "Mujahadin." Both passengers were refused admission.

- In May 2006, PNR analysis identified a high-risk traveler arriving at Atlanta Hartsfield airport from Europe. CBP officers determined that the individual's visa was issued one week prior to September 11, 2001, yet he had never traveled to the United States. The subject's passport listed him as a "flight instructor" and his reasons for traveling to the United States included the plan to "see a man in New York for two days." The individual was ultimately linked to numerous individuals who U.S. law enforcement regards as security risks and immigration violators. The passenger was denied admission.

- In May 2006, CBP officers used PNR data to target a high-risk passenger arriving from Amsterdam. Officers linked the subject to a split PNR; the second traveler was a Palestinian who previously claimed political asylum. The high-risk passenger was also identified through a known telephone number used by terrorist suspects contained within his PNR.

> Upon arrival the subject applied for admission as a Jordanian citizen and was referred to secondary inspection for further examination. The subject revealed that his purpose of travel was to visit a relative for thirty days. During the secondary inspection, the subject revealed that he had been arrested and convicted on terrorist related charges in a third country. The subject also admitted to being a former member of an organization that espoused political views and supported violent acts that include suicide bombings. The Joint Terrorism Task Force and Immigration and Customs Enforcement were contacted and responded to interview the subject. Upon completion of the interview the subject claimed credible fear of returning to Jordan. He later recanted and was expeditiously removed from the United States.

If such a system had been fully developed before 9/11, we might have been spared that tragedy. Consider this: two hijackers, Nawaq Alhamzi and Khalid Al-Midhar, appeared on a watchlist and would have been "flagged" when they purchased their tickets. Through analysis of their PNR data, we could have learned that three other hijackers - including Mohammed Atta - used the same address as Alhamzi and Al-Midhar; five other hijackers used the same telephone number as Atta; and still one other used the same frequent-flyer number. The analysis of PNR and other basic data that we use today would have flagged all nineteen hijackers as connected to Alhamzi and Al-Midhar. If we surrender this tool, we will abandon the real-time defenses that can save our citizens' lives.

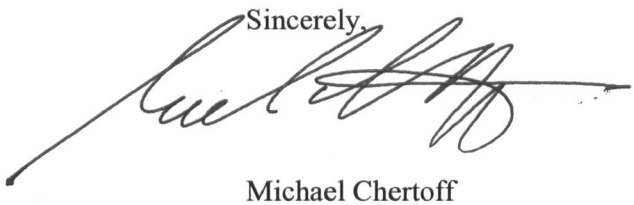
These concrete examples illustrate the necessity of analyzing and sharing PNR data. But it is also important to note the strong privacy protections in place to safeguard this information. PNR data is protected under the U.S. Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through the U.S. Congress, American courts, and internal controls such as the Department of Homeland Security's Privacy Office, Inspector General, and Government Accountability Office. In addition, our policies ensure that records pertaining to foreign nationals are properly protected.

PNR data is also used in strict accordance with U.S. law. Our officers make determinations based on relevant criteria developed from investigative and intelligence work. PNR data does not alone tell us who is and who is not a terrorist. It simply helps our officers make a more complete and informed assessment at the border to decide who warrants further scrutiny prior to entry. And PNR data is not used to create a "risk score" that remains with an individual or automatically adds a person to a terrorist watch list.

One of the central lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must break down barriers to information sharing. That same lesson must extend to our use of PNR data. We must not take this valuable counterterrorism tool away from border law enforcement professionals by limiting or restricting the kind of information sharing and analysis that has already proven effective.

I appreciate the time you have given me today to address the Committee, and I look forward to working with you as we seek new ways to strengthen international cooperation in our fight against terrorism while protecting the fundamental rights and liberties we all cherish.

Sincerely,



Michael Chertoff