INTELLIGENCE SHARING AND TERRORIST TRAVEL: HOW DHS ADDRESSES THE MISSION OF PROVIDING SECURITY, FACILITATING COMMERCE, AND PROTECTING PRIVACY FOR PASSENGERS ENGAGED IN INTERNATIONAL TRAVEL

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

OCTOBER 5, 2011

Serial No. 112–49

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

73–736 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
PETER T. KING, New York *(Ex Officio)*
JACKIE SPEIER, California
LORETTA SANCHEZ, California
BRIAN HIGGINS, New York
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Director*

CONTENTS

INTELLIGENCE SHARING AND TERRORIST TRAVEL: HOW DHS ADDRESSES THE MISSION OF PROVIDING SECURITY, FACILITATING COMMERCE AND PROTECTING PRIVACY FOR PASSENGERS ENGAGED IN INTERNATIONAL TRAVEL

Wednesday, October 5, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Long, Speier, Hochul, and Hahn.

Also present: Representative Jackson Lee.

Mr. MEEHAN. The Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today to hear testimony regarding how the Department of Homeland Security addresses the mission of providing security, facilitating commerce, and protecting the privacy of passengers engaged in international travel.

I would like to welcome everyone to today's subcommittee on counterterrorism and intelligence hearing. I look forward to hearing from today's witnesses on the value and efficacy of the Passenger Name Record program in our on-going mission to prevent terrorists and other dangerous criminals from entering the United States.

I further look forward hearing and learning about the status of on-going negotiations with our partners in the European Union with regard to the 2007—I am going to refer to this from this point forward as PNR, the Passenger Name Record, so we don't have to continue to do it, but the 2007 PNR record as well as the privacy concerns that David raised.

But before I begin, I think especially on a committee like this it is so appropriate to take a moment to recognize the tremendous victory that was achieved by our U.S. military intelligence communities in locating and killing Anwar Al-Awlaki last Friday.

Awlaki was one of the worst perpetrators of terrorism and one of the United States' most real enemies. He was involved in multiple attacks against the U.S. homeland including the Fort Dix six

plot, which occurred in my backyard; the Fort Hood attack; the Christmas day 2009 attack over Detroit; and the UPS cargo bomb which again landed in my airport. Or the airport in my district, it is not my airport.

The world is a safer place now that Awlaki is no longer a part of it.

The achievement is a great testament to the U.S. intelligence capabilities. It will send a clear message to those who seek to harm us that you won't hide, and you won't escape justice.

Now today's hearing is aimed at educating our Members, and I think many at-large, about the ways in which the Department of Homeland Security collects, protects, and uses personal information on travelers attempting to come into the United States.

Given the transnational nature of terrorism, and a desire of terrorist operatives to enter the United States from abroad, it is crucial that we act in partnership with other nationals around the world. We push it out a little bit further and make sure our skies and our ports are safe and secure from wrongful entry.

In 2007 the United States and the European Union entered into an agreement to share with one another intelligence that would help all parties identify potentially dangerous individuals before they set foot on an aircraft, thus helping to disrupt the effort of terrorists and organized crime rings.

Since 2007, the programs resulting from this agreement have proven to be an indispensible component in our strategy to thwart terrorists. In fact, in 2008 and 2009, PNR helped the United States identify individuals with potential ties to terrorism in more than 3,000 cases.

Among these was the Mumbai attack plotter, David Headley, who was arrested in Chicago after U.S. authorities accessed his PNR data from a flight he had booked from the United States to Germany. Headley since pled guilty to a separate plot to murder journalists from a Danish newspaper.

PNR data also identified Faisal Shahzad, the perpetrator of the failed Times Square bombing in May 2010, who was caught with the help of PNR as he attempted to escape the United States at JFK Airport.

In 2010, approximately one-quarter of those individuals denied entry into the United States for having ties with terrorism, were initially tied through PNR data.

Now in 2009, the European Union member states adopted the Treaty of Lisbon, and that gave greater power to the European Parliament. Thereafter, this parliament sought, under its new authority, to reject this E.U.-U.S. PNR agreement because the United States had negotiated bilateral memorandums of understanding rather than establish uniform rules with the European Union as a representative body.

In addition, some members of the E.U. Parliament have begun to criticize the agreement for not providing stricter privacy protections—and I hope that you will go in to the privacy protections that we have—even though no violation of privacy rates, or breach of security, had been reported. I hope you will develop that point as well.

The United States has been absolutely vigilant in assuring that individual privacy rights under both the U.S. and European law were respected.

As many know, last month Attorney General Eric Holder traveled to Brussels to discuss with European lawmakers the collaborative efforts between the United States and the European Union to address mutual security concerns. Holder testified before the parliament's committee on civil liberties to attempt to assuage their fears.

He argued that the debate over data protection is a purely academic one. Despite differences between the U.S. and European legal structures, both protect civil liberties effectively.

Still, DHS and other components have been involved in on-going negotiations with the European Union to amend the PNR agreement, and it has been on-going since 2009.

We have been through four rounds of such discussions. In fact they continue on these terms which were supposed to remain in effect until 2014.

Our main concern in Congress, and part of the reason we are holding this hearing today, is to ensure that negotiations with the United Nations and European Union do not impact the effectiveness of this agreement. The PNR programs have been invaluable tool in our gathering of actionable intelligence over the course of the 4 years. It is a tool we cannot do without.

The United States was built upon principles of freedom and civil liberty. This country has always been a leader among nations of upholding the rights of the individual person, and it will continue to be. It is for this reason that we must maintain our ability to prevent those who would seek to take those freedoms from us from carrying out their plans.

Privacy is a right, but so is security. One relies on the other.

I look forward to hearing from today's distinguished witnesses and on these matters.

Now, the Chairman recognizes the Ranking Minority Member of the subcommittee, the gentlewoman from California, Ms. Speier, for any statements she may have.

Ms. SPEIER. Mr. Chairman, thank you for holding today's hearing and having us focus on the PNR issue.

I would like to associate myself with the comments you made about the successful efforts by the President, the military, and the CIA in actually putting al-Awlaki to his final demise.

I would also like to welcome the witnesses here, and look forward to gaining insights into how the Department of Homeland Security uses the PNR, including how DHS protects travelers' privacy. It has got to be a key component of the utilization of this information.

It is, in fact, one of the most powerful tools that we have to combat terrorist travel. There is obviously a very important balancing that must go on.

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 of the watch lists, and who on the surface appear like any other traveler.

PNR can be immensely important in terrorism investigations. Investigators can use a terrorist suspect's past travel history to identify travel to terrorist-safe havens as well as co-travelers who may be associates, which can help to identify and disrupt the entire terrorism network.

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

But we almost missed Shahzad when he attempted to leave the country. So the question that we must ask is: What enhancements to the system have been put in place to address the vulnerabilities exposed by that near miss?

Effectively combating terrorist 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 an undue burden on the airline companies or to the traveling public is a question that must be answered.

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 for 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 United States.

"How will proposed changes to the agreement affect our screening operations?" is yet another question we must ask.

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 travelers' 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 the right to be concerned. 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, for how long, and how is it 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? How might further future modifications to the agreement 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 PNR 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 system 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?

With that, Mr. Chairman, I yield back.

Mr. MEEHAN. Thank you, Ms. Speier.

I want to have the other Members of the committee be reminded that any statements that they would like to make can be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today on this important topic.

Let me first turn to Mr. David Heyman.

He is the assistant secretary for policy at the Department of Homeland Security. Mr. Heyman is an expert on terrorism, critical infrastructure protection, bioterrorism, and risk-based security.

Previously, Mr. Heyman has served as a senior fellow and director of the CSIS Homeland Security Program where he led the research and program activities for that section.

Additionally, Mr. Heyman has held a number of Government positions, including as a senior adviser to the U.S. Secretary of Energy and at the White House Office of Science and Technology policy on National security and international affairs.

Mr. Heyman has testified before several committees in Congress and authored numerous publications, and appeared in various media outlets.

I now recognize Secretary Heyman for his testimony, and ask that you do your best to stay within the 5-minute parameters.

Thank you, Mr. Heyman.

STATEMENT OF DAVID HEYMAN, ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Thank you, Mr. Chairman, good morning Ranking Member Speier and distinguished Members of the subcommittee.

We very much appreciate the opportunity to appear before you today to discuss how the Department of Homeland Security's prescreening of passengers, and in particular the use of PNR data, plays an important role in our Nation's work to prevent and counter terrorist and criminal threats to the homeland.

Preventing terrorists from traveling to or remaining undetected in the United States remains a top priority of the Department, and I commend this committee for holding this hearing and for your support on the on-going efforts to renegotiate our agreement with Europe on the exchange of PNR data.

Ten years ago screening passengers coming to the United States was limited to the Department of State's visa process and the inspection of a person by an immigration officer at the port of entry, plus whatever processes were applied at foreign airports and by foreign governments.

If you were a terrorist seeking to come to the United States you would for all intents and purposes apply for a visa, purchase a ticket, and board an aircraft to America.

There would most likely not have been checks to see if you were a known or suspected terrorist, no checks to see if you may be a risk to security based upon behavior, no checking to see if you were traveling on a lost or stolen passport, no screening of you or your luggage for explosives, little to no security on-board the aircraft, and no checking to see if you are even admissible to the United States.

That has obviously all changed in the last 10 years.

Back then provision of advance passenger information was voluntary, and even when provided by air carriers frequently contain inaccurate and inconsistent data. There was no biometric collection of visa applicants beyond photographs, nor for aliens seeking admission to the United States. There was very limited pre-departure screening of passengers seeking to fly to the United States.

Today, a decade later, in response to both 9/11 and evolving threats and with the help and support of Congress, we have significantly adapted and enhanced our ability to detect and interdict travel threats at the earliest opportunity. PNR plays a central role in all of this.

The term PNR refers to the data an airline receives from a traveler to book and manage travel plans, and may include the traveler's itinerary, payment method, and contact information.

Just as fingerprinting was first used and became an important tool in criminal investigations in the beginning of the 20th Century, so too at the start of the 21st Century has PNR analysis become a vital tool for helping to identify terrorists and criminals.

DHS analyzes PNR provided by the airlines to help identify, detect, and thwart terrorists and criminals attempting to blend into the traveling public, and before they commit criminal acts against innocent peoples.

Our analysis of PNR data helps the U.S. Government to identify—as the Chairman has noted—over 1,700 unique suspicious activities or suspicious cases every year, and it has been vital in almost every high-profile terrorist investigation since 9/11.

PNR data analysis has been proven to be a critical tool in identifying nearly every human smuggling case involving air travel.

My colleague, Tom Bush, executive director for targeting and analysis for our customs and border patrol, will elaborate on the use and protection of PNR data international targeting programs this morning.

In addition to the Department's PNR system being operationally effective, we also can be proud of our outstanding record of data privacy protection over the past decade. To ensure the protection of privacy and civil liberties, DHS use of PNR data is subject to oversight for multiple independent bodies including the Department's chief privacy officer, the DHS inspector general, the GAO, and as well as the United States Congress.

In addition, periodic joint reviews with E.U. officials have confirmed the value of PNR data in protecting the traveling public. These reviews have confirmed our adherence to the highest data protection and privacy standards.

My colleague, Mary Ellen Callahan, the Department's chief privacy officer, is here to elaborate further on our protection and privacy programs.

Let me close by saying, over the past decade the use of PNR has evolved into a critical tool for ensuring the security of the traveling public, but also for identifying and prosecuting terrorists and criminals.

The Department has accomplished all this while also demonstrating its firm commitment to protecting the privacy of travelers. Of literally billions of passengers traveling to and from the United States over the past decade, there has not been a single breach of use of PNR and violation of established privacy protections.

In fact, the PNR system we have put in place has become a model internationally for other countries seeking to implement similar programs of which there is nearly a dozen now. We are seeing more and more countries seeking to establish their own PNR systems, including the European Union who we are in negotiations with right now.

So let me again, thank the committee for this opportunity to discuss this matter, and to helping us ensure the commitment is maintained to achieve a security with the traveling public in exchange of data to accomplish that.

I look forward to your questions. Thank you.

[The joint prepared statement of Mr. Heyman, Ms. Callahan, and Mr. Bush follows:]

JOINT PREPARED STATEMENT OF DAVID HEYMAN, MARY ELLEN CALLAHAN, AND THOMAS BUSH

OCTOBER 5, 2011

INTRODUCTION

Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security (DHS) works to prevent individuals that may pose a risk to our National security from entering the country—all while facilitating legitimate travel and commerce and protecting the privacy of individuals engaged in international travel.

Specifically, I want to highlight the Department's pre-screening of passengers, and in particular, the use of Passenger Name Record (PNR) data in our work to prevent and counter terrorist and criminal threats to the Homeland. PNR data and analysis play a unique role in enabling the U.S. Government to identify both known and unknown threats. Recent cases underscore the vital benefit of PNR and reflect its value today—a value that has grown in recent years as the Department has improved and expanded its data matching and processes. We have been able to advance the development, implementation, and use of this tool, while also protecting travelers' data and privacy.

Other countries, recognizing the utility of PNR, have expressed interest in developing their own PNR systems for screening travelers. Our on-going negotiation with the European Union over how PNR from flights with ties to the European Union is handled by DHS is one manifestation of our ability to advance security, data protection, and privacy together. I commend the subcommittee for holding this important hearing on this topic.

Multiple Layers of Defense

Since 9/11, we have learned that the exercise of immigration and border security authorities can be powerful resources used to identify and thwart terrorist operations at the earliest opportunity. We have significantly adapted and enhanced our ability to detect and interdict threats at the earliest opportunity by instituting a layered aviation and border security architecture, incorporating both seen and unseen assets.

Accordingly, we have strengthened our security and screening at points:

- During the travel planning phase, when a traveler seeks a visa or authorization to travel;

- Just prior to travel, when a person seeks to board an aircraft at a point of departure; and
- During travel, when a person seeks to enter the United States.

PNR is one of five automated systems that assist the Department in identifying travelers likely to pose a risk. The five reinforcing systems are: PNR; the visa application process (conducted by the Department of State and supported by DHS); the Electronic System for Travel Authorization (ESTA) for travel under the Visa Waiver Program; the Advance Passenger Information System (APIS), and; Secure Flight. These are the systems DHS uses to begin conducting screening before an aircraft's departure and function in conjunction with physical security procedures such as checkpoint screening.

PASSENGER NAME RECORD—PNR

The term PNR refers to the data an airline receives from a traveler to book and manage travel plans, and may include the traveler's itinerary, payment method, and contact information. In light of the lessons learned from 9/11 about identifying and preventing terrorists traveling into and out of the United States, Congress mandated that carriers make PNR data available to the U.S. Government in the *Aviation and Transportation Security Act of 2001* (ATSA, Pub. L. 107–71). Presently, all carriers flying to and from the United States provide DHS with PNR pursuant to ATSA and DHS implementing regulations. DHS analyzes PNR provided by the airlines to identify terrorists and criminals attempting to blend into the traveling public before committing criminal acts against innocent people. Our analysis of PNR data, reinforced through cooperation with Federal partners, has helped to identify approximately 1,750 unique suspicious cases every year, and has been vital in many of the United States' most well-known terrorism investigations since 9/11.

To ensure the protection of privacy and civil liberties, DHS' use of PNR data is subject to oversight from multiple independent bodies, including the Department's Chief Privacy Officer, the DHS Inspector General, and the Government Accountability Office, as well as the U.S. Congress. In addition, periodic joint reviews with E.U. officials have confirmed the value of PNR data and our adherence to the highest data protection and privacy standards. The findings of these joint reviews are available on-line on the DHS and E.U. websites. Over the last decade, the Department has demonstrated its firm commitment to protecting the privacy of travelers. Of the literally billions of passengers traveling to and from the United States during the past 10 years, there has not been a single data breach or privacy violation of the PNR data.

CONTINUED THREAT/RISK OF TERRORIST TRAVEL

This year witnessed the deaths of both Osama bin Laden and Anwar al-Awlaki, as well as the 10-year anniversary of the deadly terrorist attacks of 9/11. As we reflect on the past decade, it is important to remain cognizant of the continued, evolving threat of terrorism to the traveling public. Since 9/11, the threat has changed to include not only large-scale attacks but also smaller operations with potentially catastrophic effects, including the continued targeting of the aviation sector. One of the most important responsibilities of government is the protection of its citizens, a duty this Department well recognizes and takes seriously. Passengers have a right to privacy and protection of their civil liberties and personal information, but also have a right to know that their government is doing everything it can to ensure their safety and security when they board an airplane. It is necessary, therefore, to ensure the continued use of proven and effective security measures. PNR is a proven asset in the fight against terrorism and other transnational crimes.

EVOLUTION OF U.S. PRESCREENING EFFORTS SINCE 9/11

Ten years ago, screening of passengers coming to the United States was limited to the Department of State visa process, if applicable; the inspection of a person by an immigration officer at the port of entry; and any processes applied at foreign airports by foreign governments. Provision of advance passenger information was voluntary. There was very limited pre-departure screening of passengers seeking to fly to the United States, and there was virtually no screening of any kind for domestic flights beyond airport checkpoints.

Today, in response to both 9/11 and evolving threats, and with the help and support of Congress, DHS has significantly adapted and enhanced its ability to detect and interdict threats at the earliest opportunity, including through the access to and analysis of PNR data as mandated by Congress. PNR data are analyzed in conjunction with other screening tools such as visa applications, the Advance Passenger Information System, and the Electronic System for Travel Authorization (ESTA). DHS

analysis of PNR data is an indispensable layer in a comprehensive approach to security. Each tool plays a unique role in the screening process. ESTA and the visa issuance process (depending on the country and traveler) allow us to prevent a known criminal or terrorist from preparing to travel. Secure Flight and APIS help DHS decide how the carriers and CBP officers, respectively, should handle travelers as they prepare to board. PNR data further enable this decision with additional and earlier information. APIS and PNR then help DHS decide who warrants a secondary examination upon arrival. In all cases, trained DHS personnel review and analyze the results of these automated systems.

As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons this country has to counter terrorist operations. Terrorists travel in order to: Identify and engage in surveillance of potential targets; plan attacks; receive training on tactics and operations; collect and transfer funds and documents; and communicate with other operatives. Every step along this pathway presents a vulnerability for would-be attackers, who must come out of the shadows and interact with the traveling public, the travel industry, and immigration and border security officials. At some point along the travel pathway, for example, many terrorists cross international borders—a step that often necessitates submitting advance passenger information, using a passport, and undergoing screening by immigration and border officials while at ports of entry.

THE ROLE OF PNR DATA WITHIN THAT SYSTEM

PNR data analysis can help identify individuals up to 72 hours prior to departure, including watch-listed individuals, non-watch-listed co-travelers, and terrorists or criminals adopting known illicit travel patterns. DHS is able to link previously unknown terrorists and criminals to known terrorists or criminals by matching contact information, flight patterns, and other data. After this analysis is complete, DHS works with foreign and industry partners to interdict illicit travelers prior to boarding or prioritizes resources for their inspection at U.S. ports of entry. PNR data collection and analysis also support terrorist and criminal investigations, including the three most prominent U.S. terrorist investigations in 2009 and 2010. Further, PNR served as a critical tool in supporting United States Government efforts to investigate 9/11 threats over the tenth anniversary weekend.

The retention of PNR data after a flight allows DHS to unravel more complex plots by looking at travel practices over time. Data that does not appear to be relevant at the time of travel can be critically important when tied to a specific case later. Remember that the 9/11 plot was originally conceived in the early 1990s; an attempt on the World Trade Center occurred in 1993, and the actual 9/11 plot planning and execution began in earnest in 1996. This included numerous dry runs and practice flights, as well as travel for recruitment and planning. Retained travel data was important in securing convictions by the Department of Justice in a number of recent counter-terrorism cases, including the conviction of Mumbai plotter David Headley.

Identifying Unknowns

Following 9/11, the United States Government collected intelligence on al-Qaeda and its affiliate networks and established the FBI's consolidated Terrorist Screening Database (TSDB) of known or suspected terrorists. Today, we check travelers to the United States against the TSDB, no matter what mode of transportation they plan to use to come to the United States.

As DHS has seen in recent cases, however, intelligence and law enforcement agencies may have limited or no derogatory information about individuals who pose a real risk to the United States. In fact, we know that some terrorist groups are deliberately looking to recruit individuals who are specifically unknown and can remain undetected by heightened security measures. Fortunately, PNR data analysis, particularly of historic records, allows us to help identify individuals who may be unknown to us as terrorists or criminals, but exhibit a pattern of behavior that is consistent with known or suspected terrorist or transnational criminal behavior. For example, a few years ago, two organized crime syndicates in Latin America devised a simple and effective way to smuggle kidnapped children into the United States for sale. They would pay women to fly to the United States with their own children's legitimate passports but with kidnapped babies. The women would then return alone. By looking for such a pattern in PNR records over a number of years DHS arrested 11 smugglers, removed 10 criminals and identified 37 victims. The same technique of analyzing travel patterns has proven effective against a myriad of crimes and terrorism.

At the same time, DHS realizes that sometimes innocent travelers may adopt what may appear to be suspicious patterns. As a result, DHS has established auto-

mated procedures so if a traveler is repeatedly flagged for further inspection and found not to pose a risk, DHS will automatically "de-flag" the traveler in the future. Further, all pattern-based rules are evaluated quarterly by the DHS Chief Privacy and Civil Liberties Officers for effectiveness and appropriateness. A Customs and Border Protection (CBP) officer, however, may still determine that a closer inspection is warranted, depending on the individual circumstances and travel.

Early Identification—Activation of IAP Teams

CBP stations Immigration Advisory Program (IAP) officers at certain foreign airports to work with airlines and foreign officials to identify high-risk and improperly documented travelers before they board aircraft bound for the United States. At the invitation of foreign partners, IAP officers make "no-board" recommendations to airlines on the basis of passenger data analysis and a review of individual travel documents. To be most effective, several hours before a flight is scheduled to depart, an IAP officer must know who will likely be on a flight and whether they warrant further exam prior to departure. Frequently, PNR data analysis is the first information IAP officers receive to assist in making these determinations. CBP's National Targeting Center—Passenger (NTC–P) analyzes PNR data received up to 72 hours prior to departure and provides recommendations to the IAP officers. NTC–P later validates this analysis with APIS closer to departure. IAP officers are currently posted at 10 airports in 8 countries, and have recommended, in part based upon PNR data, a total of 2,875 no-boards in fiscal year 2011, including 9 No-Fly hits, 74 confirmed Terrorist Screening Database matches, and 109 cases of fraudulent document use.

EXAMPLES OF PNR EFFECTIVENESS

Headley, Zazi, Shahzad

I would like to take a little time to discuss some of the high-profile cases where PNR data analysis has been instrumental in critical National security investigations and prosecutions. As background, I mentioned earlier that analysis of PNR data have proven to be the critical tool for annually identifying around 1,750 suspicious cases. PNR data have also aided nearly every high-profile terrorist investigation, including: David Headley, who pled guilty for his role in the 2008 Mumbai terrorist attacks; Najibullah Zazi, who pled guilty to plotting to bomb New York City subways; and Faisal Shahzad, who pled guilty to attempting to detonate a car bomb in New York's Times Square. Just as fingerprinting was first used and became an important tool in criminal investigations in the beginning of the 20th Century, so too at the start of the 21st Century has PNR analysis become a vital tool in terrorist and transnational criminal investigations. DHS has also relied on PNR data analysis in nearly every human smuggling case involving air travel.

The case of Faisal Shahzad clearly demonstrates the effectiveness of DHS's prescreening programs. Early in this investigation, the Federal Bureau of Investigation (FBI) learned of Shahzad's cell phone number, but had little additional information. Through good interagency cooperation, the FBI asked DHS if it had encountered any individual who reported this phone number during border crossings. DHS searched its PNR database for the phone number, identified Shahzad, and learned other information he had provided to DHS. DHS then provided the additional data to the FBI. Later, Shahzad attempted to flee the United States, but DHS's analysis of departing passenger data identified him before departure and DHS removed him from the aircraft.

STRONG RECORD OF PRIVACY PROTECTION

DHS provides robust privacy protections and strict safeguards over PNR data. Through a combination of law, policy, and oversight, DHS ensures its compliance with stringent standards of privacy and security in the collection and use of PNR data. DHS applies fair information practice principles to its collection and use of PNR, including data integrity, data security, purpose specification, auditing and accountability, individual access, and redress. Moreover, the Department is firmly committed to transparency when it comes to informing our partners and the public about its mission, including how we use and safeguard personally identifiable information such as PNR data.

By leveraging the Congressionally-mandated authorities of the DHS Chief Privacy Officer, DHS is working diligently to assure all U.S. and international travelers that the highest standards are being applied to the protection of their personal information. The Chief Privacy Officer has managed two internal audits of DHS's use of PNR data and coordinated two joint reviews with the European Union since 2004. When preparing for the joint review that took place in February 2010, the DHS Privacy Office spent approximately 10 weeks of employee time analyzing and assessing

DHS collection and use of PNR data and published two public reports related to that assessment. The reports from these audits are publicly available on the websites of the DHS Privacy Office and the European Union. The DHS Privacy Office found, and the European Union acknowledged, that there has not been a single incident involving the unauthorized use of PNR data.

Individual travelers have many opportunities to learn how DHS handles PNR data. The PNR data rule, System of Records Notice, and Privacy Impact Assessment are all available for public review and comment. In addition, individuals, both U.S. and non-U.S. citizens, have multiple opportunities for access and redress. The *U.S. Freedom of Information Act (FOIA)* applies equally to U.S. citizens and non-U.S. citizens. Anyone can request his or her PNR data directly from DHS; DHS receives and answers these types of requests routinely. If the traveler seeks to change or delete information contained in his/her PNR, he or she can submit a request to DHS and changes deemed appropriate will be made. U.S. and non-U.S. citizens alike also have access to the DHS Traveler Redress Inquiry Program (DHS TRIP) to correct or amend records. More information on these programs can be found at *www.dhs.gov/privacy.*

U.S.-E.U. PNR AGREEMENTS

Despite this operational and privacy success, last year, the European Union sought to re-negotiate our bilateral PNR Agreement to obtain further reassurance that data with ties to Europe is being handled properly by the United States. To protect U.S. industry partners from unreasonable lawsuits, as well as to reassure our allies, DHS has entered into these negotiations.

The Agreement currently in force provisionally, negotiated in 2007, is not scheduled to sunset until 2014. The Agreement is operationally sound, but it is subject to ratification by the European Parliament, which instead directed the European Commission to renegotiate the Agreement. As a matter of good faith and out of respect for our E.U. partners and their evolving political structures following enactment of the Lisbon Treaty, Secretary Napolitano subsequently agreed to negotiate a new agreement only if the new text would not degrade the operational effectiveness of the 2007 Agreement and would permit additional security enhancements where necessary. We commenced the latest negotiations on December 4, 2010. As such, the United States is currently in its fourth negotiation over PNR with the European Union in 9 years—effectively a decade of negotiation.

The Department is committed to concluding a new PNR agreement, first and foremost a security agreement, which upholds vital public interests in both security and privacy. We reached agreement with the European Commission for such a text on May 16, 2011. The text is an improvement over the 2007 Agreement, it protects both security and privacy and U.S. and European interests, it provides all relevant parties with legal certainty, and it is a reliable framework for an enduring deal.

U.S. and E.U. negotiators worked to respond to the European Parliament's criticism of the 2007 Agreement, to improve passenger security and to provide air carriers a legally certain operating environment. To build support for this approach, DHS has met repeatedly with not only the European Commission, which negotiates on behalf of the European Union, but also with key Committees and Members of the European Parliament and representatives of individual Member States. The new agreement is clear, detailed, and transparent—in ways that some critics in Europe felt the previous Agreement was not. The text of the draft agreement defines key terms such as "terrorism," and "transnational crime" consistently with United States, European Union, and international norms. A data retention period acceptable for U.S. security purposes is maintained, with additional safeguards to ensure privacy and data protection. The new agreement will require travel information to be transmitted to DHS with greater lead time than provided for in the 2007 Agreement, and thus will provide for greater analysis earlier in the passenger travel lifecycle. It also provides for a new method of data transmission ("real-time" push). By restricting data transmission to the minimum necessary while ensuring data accuracy, the real-time push method of sharing data will enhance security and privacy protection at the same time. Lastly, the new agreement will expand opportunities for police and judicial cooperation between the U.S. and E.U. authorities.

I want to thank this committee for its interest and support in our negotiations with the European Union. With the conclusion of PNR negotiations with the European Commission and, we hope, forthcoming signature and then support from the European Parliament, the United States and European Union will have made progress in strengthening the previous PNR Agreement from a privacy and security perspective. Success will be the result of 9 months of intense negotiations and build

off 9 years of dialogue on how best to facilitate safe transatlantic travel and protect individual privacy.

By all accounts, the new text is stronger than the 2007 Agreement; it addresses all E.U. concerns raised with the U.S. negotiating team, while also preserving and in some cases improving critical U.S. operational interests. We must build on our historic relationship, values, and interests, as we seek action by the European Commission, the European Council, and the European Parliament to finally conclude this PNR Agreement, which is without a doubt better for enhanced security, as well as for improved data and privacy protections.

CONCLUSION

Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee, we look forward to working with you as we explore opportunities to advance our cooperation with our European partners to counter terrorism and transnational crime. Thank you again for this opportunity to testify. My colleagues and I are happy to answer your questions.

Mr. MEEHAN. Thank you, Mr. Heyman, for your testimony and for your good work and service in your current position.

Next, the Chairman would like to recognize Ms. Mary Ellen Callahan, who was appointed the chief privacy officer and chief freedom of information officer by DHS Secretary Napolitano in March 2009.

In her role as chief privacy officer, Ms. Callahan is responsible for evaluating Department-wide programs, systems, technologies, and rulemakings for potential privacy impacts, and for providing mitigation strategies to reduce any privacy impact.

She and her staff have extensive expertise in privacy laws both domestic and international that help inform privacy policy development both within the Department and in collaboration with the rest of the Federal Government.

Prior to joining DHS, Ms. Callahan was a partner with the law firm of Hogan & Hartson where she specialized in privacy and data security law.

In 2011, Ms. Callahan received the Federal 100 award which recognizes individuals in Government and industry that make significant contributions to the Federal I.T. community.

I now recognize Ms. Callahan to testify for 5 minutes.

STATEMENT OF MARY ELLEN CALLAHAN, CHIEF PRIVACY OFFICER, THE PRIVACY OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. CALLAHAN. Thank you very much.

Good morning, Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee.

My name is Mary Ellen Callahan. I am the chief privacy officer at the Department of Homeland Security.

As the Chairman acknowledged in his introduction, I am responsible for evaluating Department-wide programs, systems, and technology for potential privacy impacts including the Department's use of passenger name records—and I will take your cue and call it PNR—through Customs and Border Protection's Automated Targeting System. I will also refer to this as ATS.

DHS provides privacy protections and strict safeguards over PNR data. DHS ensures its compliance with stringent standards of privacy and security in the collection of use of PNR.

DHS applies fair information practice principles to its collection and use of PNR including data integrity, data security, purpose

specification, auditing and accountability, individual access, and redress—the principles which I will detail in my testimony this morning.

Moreover, the Department is firmly committed to transparency when it comes to informing our partners and the public about its mission, including how we use and safeguard personally identifiable information such as PNR data.

My office has managed three internal audits of DHS' use of PNR data and coordinated two joint reviews with the European Union since 2004. For example, when preparing for the joint review that took place in February 2010, the DHS privacy office spent approximately 10 weeks of employee time analyzing and assessing DHS collection and use of PNR data, and published two reports totaling 65 pages related to that assessment.

My staff conducted multiple interviews, reviewed the PNR data use in sharing audit trails, and SOPs for ATS.

We also reviewed the logs in ATS associated with whether sensitive data had ever been accessed by DHS. It had never been accessed.

Through these two joint PNR reviews, the DHS privacy office found, and the European Union acknowledged, that there has not been a single privacy incident or data breach involving the unauthorized use of PNR data.

These public compliance reviews conducted by my office confirm the original intent of the data collection, and provide public assurance that the information is being used for the purposes for which it had been collected. The pattern-based rules that are referred to in our written testimony, that DHS employees are also subject to my review, as well as that of the officer for civil rights and civil liberties, and the Office of General Counsel.

On a quarterly basis, we review these pattern-based rules, the underlying intelligence that supports the rules, and the impact effectiveness and efficacy of the rules themselves.

This periodic oversight and review allows DHS to perform its border security task in a privacy-protective way.

In addition to my statutory authorities related to privacy compliance, the DHS privacy office is involved in data governance and information sharing in the Department through the chief information officer and his counsels, departmental compliance with FISMA, I.T. budget review, and the information sharing and governance board.

This type of integrated, ex-anti and ex-post assessment and review by the DHS privacy office is one of the virtues of the senior position my office has within the Department, with visibility and oversight through the data life-cycles of DHS programs, systems, and technologies.

As the committee knows, I have had the pleasure of serving as the Department's chief FOIA officer as well. One of the ways the Department supports the privacy fair information practice of individual participation is to provide travelers with multiple opportunities for access and redress.

FOIA applies equally to U.S. citizens and non-U.S. citizens. Anyone can request their PNR directly from DHS. DHS receives and answers these types of requests routinely. Based on a recommenda-

tion by the European Commission in the 2010 review, we now track that number discretely.

Since April 2011, DHS has received approximately 220,000 FOIA requests from around the world. In that same time period, we have received 69 FOIA requests from travelers seeking their PNR records.

If a traveler seeks to change or delete information contained in his or her PNR, they can submit a request to DHS and changes deemed appropriate will be made. The administrative appeals through my office are also available.

This existing opportunity was strengthened through the Department record amendment policy that was released earlier this year.

Furthermore, U.S. citizens and non-U.S. citizens alike have access to the DHS traveler redress inquiry program to resolve travel-related inquiries such as the use of PNR.

In sum, the DHS' collection and use of PNR, and my office's involvement throughout the PNR life-cycle, demonstrates the Department's commitment to embedding privacy principles within the Department's operations.

I look forward to your questions, sir.

Mr. MEEHAN. Thank you, Ms. Callahan.

Last, let me turn to Mr. Thomas Bush, the executive director of automation and targeting for the Customs and Border Protection Office of Intelligence and Investigative Liaison.

Mr. Bush and his staff are responsible for assessing and reporting the threats that the United States Customs and Border Patrol faces through research, evaluation, and dissemination of trend analysis, intelligence alerts, and assessments.

Mr. Bush began his career as a program analyst for the Department of Defense strategic defense initiative and entered the United States customs service in 1994.

In 2006 Mr. Bush joined the Office of Antiterrorism where he acted as executive director prior to the establishment of the Office of Intelligence and Operations Coordination in 2007.

His numerous honors include the 1998 Commissioner's Unit Citation Award and the 2003 Commissioner's Annual Award for Innovation, and the 2008 Secretary's Award for Excellence.

I now recognize Mr. Bush to testify for 5 minutes.

Mr. Bush.

STATEMENT OF THOMAS BUSH, EXECUTIVE DIRECTOR OF AUTOMATION AND TARGETING OFFICE OF INTELLIGENCE AND INVESTIGATIVE LIAISON, CUSTOMS AND BORDER PROTECTION

Mr. BUSH. Good morning Chairman Meehan, Ranking Member Speier, distinguished Members of the subcommittee. Thank you for this opportunity to provide background on PNR today.

PNR is the data that an airline receives from travelers to book and manage their reservations. This can include the traveler's itinerary, payment method, and contact information.

It is one of our most important tools in the on-going fight against terrorism, as well as narcotics smuggling, human trafficking, and other transnational crime.

I will address how we get this data, how we use it, and how it has helped us in the past.

CBPs predecessors, the U.S. Customs Service and the Immigration and Naturalization Service, began receiving PNR data from commercial airlines on a voluntary basis in the early 1990s. The carriers recognize that working closely with U.S. law enforcement to intercept high-risk travelers would in turn yield benefit for enhanced security on their flights.

Shortly after September 11, 2001, Congress began mandating that the airlines provide PNR to U.S. Customs Service, now CBP. Since then, CBP has had electronic access to the PNR data of every airline with an electronic reservation system operating international flights to and from the United States.

I would also like to add that CBP works closely with our partners in the Department of Homeland Security's oversight offices, the chief privacy officer, and the civil rights and civil liberties officer to ensure transparency in how we use PNR at CBP.

We also have established clear guidelines for our officers and what they can and cannot do with the data. Not every employee in CBP needs to have access to PNR, but those that do respect PNR as a powerful tool in their decision-making process.

CBP maintains PNR in our automated targeting system or ATS. The system parses the data into discrete elements, analyzing it in conjunction with other DHS traveler holdings. This allows CBP officers and analysts to use a variety of information, to identify those travelers posing the highest risk before they board airplanes overseas.

CBP officers and analysts use PNR in conjunction with other data and law enforcement intelligence information to establish risk-based scenarios for the interception of previously unknown high-risk subjects—in other words, those not on the watch list. These scenarios, or pattern-based rules, allow officers to make faster and better-informed decisions about which travelers to interview and secondary examination.

PNR data is also useful to trend analysis. It is unique and it allows CBP to see a traveler's full itinerary and contact information such as phone numbers and e-mail address. This can be very powerful in establishing connections with other travelers who may arrive from different locations or different times, and who may appear to be otherwise unconnected.

I will cover a few of our success stories.

One important example of it is the case of Najibullah Zazi. You may recall Zazi as the al-Qaeda-trained operative who planned to explode improvised explosive devices in New York City's subway system.

Using PNR data, DHS and CBP worked closely with the FBI to cross-check the names of his co-travelers against open counterterrorism cases inside the United States, and determined his co-travelers were being trained during the same trips to Pakistan in the same training camps.

Zazi was arrested on September 19, 2009 and the information from his PNR records were used in his questioning and his indictment. Zazi pled guilty in February 2010.

Another example of CBP's ability to fully leverage PNR holdings—specifically about those we have very little information or those we call the unknowns.

Law enforcement intelligence information implicated a specific person in the plotting of the 2008 Mumbai attacks as well as the possible attacks against a Danish newspaper office. Starting with the very common first name, David, a partial travel itinerary, and a very vague travel time frame, CBP was able to review its PNR data in connection with other DHS databases.

Within 24 hours CBP was able to provide the FBI with the person's full name, address, passport number, travel history, and other information useful to law enforcement pursuing him. You may know that person as David Headley who pled guilty in March 2010.

A third example of how CBP's use of PNR and has been successful also demonstrates when we receive the data.

In the case of Faisal Shahzad, who attempted to use the car bomb in Times Square in May 2010, CBP used PNR in the first place to target him on his flight returning from Pakistan. It was also used to intercept him when he tried to flee the plot after it was unsuccessful.

After a stay in Pakistan, in which was later determined Shahzad underwent terrorist training, Shahzad arrived in the United States and was flagged for screening based on information in his PNR. CBP conducted an examination and released him after finding no reason to further detain him.

After the failed attack, the FBI, in coordination with DHS, learned of Shahzad's identity from a phone number in his attempt to purchase the car that was linked to the PNR data, and our reporting on that examination.

Based on previous information, CBP created travel lookouts on Shahzad which enabled us to intercept him before he hurriedly booked his PNR in an attempt to leave the United States on a flight out of JFK.

Shahzad confessed and was sentenced to life prison in June 2010.

Two other examples that are in human smuggling are cases in Korea of sex trade—they also were connected to Sri Lanka. PNR was used for us to target the travel routes and the travel agencies used by those perpetrators in November 2009.

A separate human smuggling case working with Interpol, we were able to use PNR data to detect payment address information and e-mail information that connected to Eastern European human smuggling cases. This was in August 2009.

PNR uniquely and solely provides CBP with the ability to identify the true point of origin for travel. Without it CBP often mistakes the origin of travel at that last point of departure to the United States—take an example for Heathrow versus an originating travel in Pakistan.

PNR also allows CBP to see all the stops along the way.

PNR also affords CBP the opportunity to determine suspicious booking and payment methods such as last-minute ticket purchase, cash tickets, or one-way tickets.

Mr. MEEHAN. Mr. Bush, can I ask you—these are all good things and perhaps these are some of the things you can develop for us in your testimony.

Do you have a closing observation for your direct testimony?

Mr. BUSH. Other than I just noticed I was over. I apologize.

Mr. MEEHAN. I can see you——

Mr. BUSH. Part of the excitement.

Thank you, sir.

Mr. MEEHAN. It does. It is interesting stuff.

Particularly, you are getting a chance to layout your trophy case and I think it is a significant record.

I want to thank each of you for your testimony here.

First, how inherently important it is because the record demonstrates the things that have been accomplished by virtue of the work that has been done with PNR.

Second as you have testified here today, each of you in different parts there is a lot of work that has gone into protecting the integrity of this information, and the audits have shown that we haven't had violations.

With that premise, we really do want to find the balance of assuring privacy while protecting the safety of Americans traveling.

So, Mr. Heyman, let me start with you because this is the kind of a thing that if you aren't close to it and you drill down to it, you know, just the terminology can overwhelm you.

Effectively, what kind of information are we using when we are engaged with PNR?

Isn't it in many ways the kind of information that the people should have an expectation that they are already currently sharing? It is just using that information in a more effective manner than we have in the past.

Mr. HEYMAN. Thank you, Chairman.

You are absolutely right. The balancing act that we have sought to accomplish, and I think frankly effectively have, is the balance that says passengers have a right to privacy and protection of their civil liberties and personal information.

But when they get on the airplane they also have a right to know their Government is doing everything they can to make sure that that flight is going to be safe. We do that through a number of different things that I have outlined, but included and most important, the PNR record.

The PNR record is basically the information that you provide an air carrier when you book a travel plan. So it is your seat number. It is your destination. It is your routing.

It is perhaps how you purchased the ticket. There are about 19 types of fields that are included and include personal information such as your name and——

Mr. MEEHAN. But not inherently private information per se, right?

Mr. HEYMAN. Well, I will let my privacy officer speak to the specifics about how privacy is accounted for. But it is information that you share with the airlines and then they share it with the Government for the purposes of the evaluation about whether an individual presents a risk getting on that aircraft.

We take that responsibility quite seriously. We have data protection for ensuring that only the information of those 19 fields are preserved.

The specifics about sensitive information that people are concerned about, we do not use that. It is our policy not to use sensitive information——

Mr. MEEHAN. Well, let me drill down to that for a moment because that is the essence of what we are really talking about, I think.

We have demonstrated over a course of period of time the effectiveness of PNR and the importance that it plays. You have also been able to create a record in which it has withstood scrutiny up to this point in time.

So what is really at play here with the European Union now coming back and challenging what has been a program which I am presuming has not only worked effectively, but my assumption is you developed more fields of information that its effectiveness only grows?

Mr. HEYMAN. Well, that is a great question.

What is at play? There is a lot of play here, some of it having to do with institutional reform in Europe post-Lisbon where the parliament now has a responsibility for approving agreement.

Previously the pathway to an agreement with the United States would be the commission negotiates an agreement and member states sign off on it. Now, the parliament also must vote on it. Seven-hundred-plus members of the European parliament will vote thumbs up or thumbs down.

Parliament for the last decade or so has made past resolutions in Europe requesting and urging the commission to provide more for data protection on these types of information-sharing agreements.

Now that they have an opportunity to vote up or down in this past year, they requested that the commission come back to the United States and seek a renegotiation of the——

Mr. MEEHAN. The point of it is, individually many of these member nations have not only appreciated the significance of the protections afforded to safety, but they have agreed and participated with you in the zones of information that should be shared. Is that right?

Mr. HEYMAN. In fact, yes. I believe it is 23 or 24 of the 27 member states ratified the 2007 or re-passed the 2007 agreement.

Mr. MEEHAN. Do we share information with them in a return capacity because there are people that fly through airlines that either go through the United States or from the United States to their countries?

Mr. HEYMAN. Yes. We may on a case-by-case basis share information. At this point the Europeans as a group don't have a PNR system. They proposed one which may take several years to stand up. Some member states—the Brits in particular—have begun to stand up their own PNR system in which case we would have that type of exchange.

Mr. MEEHAN. Well——

Mr. HEYMAN. Protected also—protected with the same data protection and privacy protections that we seek in our own agreements.

Mr. MEEHAN. My time has expired for now. But I know that there is an interest in the broad spectrum that all of us will—have to share.

So I turn it over to the Ranking Member, Ms. Speier.

Ms. SPEIER. Thank you, Mr. Chairman.

So let me follow up on the Chairman's questioning.

Does the 2007 agreement stay in place pending the negotiations on the 2011 agreement?

Mr. HEYMAN. Yes, it is provisionally in effect.

Ms. SPEIER. All right. We prefer the 2007 agreement to the 2011 agreement?

Mr. HEYMAN. Well, let me just give a little background on—Secretary Napolitano, when she agreed to renegotiate the agreement, agreed with two fundamental principles that we must adhere to. The members here are part of the negotiating team here—your witnesses.

So No. 1, she directed us that we have to maintain the same operational effectiveness as 2007. So there is no degradation in existing operational capabilities. The 2007 agreement provides us with exceptional operational capability.

No. 2, that a new text must permit additional security enhancements where necessary or appropriate, so we have been given guidelines or direction that we will have no degradation and operational——

Ms. SPEIER. Mr. Heyman, excuse me for interrupting.

I am trying to get to what the crux of the issue is with the 2011 agreement.

Would you say that the expectation of the European Union to have greater privacy protections is what is stalling the negotiations?

Mr. HEYMAN. The Europeans seek—what has stalled—the negotiations have proceeded as directly as we can. We concluded what we believe is a good text in May this past year.

They have a number of institutional hoops that they must go through. The commission must now get the member states onboard. The member states then pass it, and they have to give it to the parliament. There are some institutional things that must get accomplished.

But as far as we are concerned with perhaps a couple of other discussions, we are pretty much satisfied with the text as created in May 2011.

Ms. SPEIER. So there are no disputes pending?

Mr. HEYMAN. The Europeans have to go through their own institutional requirements, and so there is still discussions going on.

Ms. SPEIER. Okay. Can you just tell me if there is anything outstanding?

Mr. HEYMAN. From the European side there are, yes.

Ms. SPEIER. Okay. What are they?

Mr. HEYMAN. The Europeans have a legal opinion that has been put forward by the commission that says that the May text that was leaked to the public is not proportionate, which is a standard by which data protection and data use must be adhered to.

So, they are working through that challenge right now. We are open to hearing their proposals for how to fix that problem.

But it is on the European side.

Ms. SPEIER. What do you mean by proportional?

Mr. HEYMAN. So—why don't you——

Ms. CALLAHAN. The proportionality is a concept that is in the European law particularly vis-á-vis the member states to the European Union. It is one that has been incorporated into the data protection or privacy directive of 1995.

Proportionality is actually a concept that has multiple meanings within Europe. One meaning is you should only take the information that you need in order to do your job. So the number of fields that you collect from the airline, the 19 fields that Mr. Heyman spoke about.

Another concept of proportionality that we have heard discussed is that you only collect information from the people that you need to collect the information from. From, for example, the bad guys, from the criminals.

Now that of course, as Mr. Bush elaborated on we don't know who all the bad guys are. We have unknown terrorists out there, and so that is not necessarily possible.

Then there is proportionality in terms of the scope of the enforcement and the application.

Each time we talk about proportionality, we hear a different definition. So the definition in European Union law is quite broad, which is why to say that the, "agreement" is not proportionate is difficult to pin down in terms of how to——

Ms. SPEIER. Okay.

What are the 19 fields? Can someone just rattle those off for us?

Ms. CALLAHAN. Mr. Bush.

Mr. BUSH. I can try to do most of them, ma'am, and get you——

Ms. SPEIER. All right. I have got 30 seconds so——

Mr. BUSH. Travel itinerary, which covers a few of the 19 fields: Name, date of birth, payment information, e-mail address, phone number. If you have associates, co-travelers on your ticket, you are sharing, travel agency, travel agency address.

Ms. CALLAHAN. Co-chair.

Mr. BUSH. Co-chair if it splits. So if United needs to share with another airline as an example. I think that covers—bags and seat assignment.

Ms. SPEIER. All right, thank you.

Mr. BUSH. We can get you the full details.

Mr. MEEHAN. Thank you, Ms. Speier.

The Chairman now recognizes the gentlelady from California, Ms. Hahn.

Ms. HAHN. Mr. Chairman and Ranking Member Speier, this has been a very interesting hearing. Thank you for your testimony.

It is certainly—and, you know, I have a statement that I can enter into the record. I won't give it now.

But clearly PNR is an important tool that I think we use in this country to clearly, as was stated, to connect the dots. I guess the key is making sure we have the right dots, and then the real work begins on connecting those dots.

But we have certainly had some pretty impressive success stories to tell which I think is important.

You know, reading some of the background materials, I think the real problem is parliament. You know, when you read some of the quotes from the members of parliament, they are the ones that look like they could very well veto this or block it.

It doesn't seem like there is some real instances of abuse that they can point to after we have collected this information. But it is just a basic overall belief that data collection has sort of gotten to an extreme, and privacy, just on that basis, for them it sounds like to be violated.

So I think that is going to be the real issue—is their parliament.

You know, one of the things—you know, my district in California borders Los Angeles International Airport. It also borders the Port of Los Angeles.

Now, I am wondering—you know, the airport police in many of our airports in this country, certainly are sort of a separate law enforcement agency. I am wondering how this information is communicated to our airport police and vice versa—our airport police, agencies across this country in an information-sharing loop with the Department?

The other thing I was certainly wondering, it is always my concern is I think our real vulnerable points of entry into this country are our sea ports.

Wondering, does this also include—does the PNR also include passengers who would be coming into this country through cruise ships, for instance? Is that an area of concern?

Because it is for me, and wondering where we are in really looking at information for those who come into this country on, you know, some major cruise ships certainly from Europe—so just kind of two questions.

Mr. HEYMAN. Thank you, Congresswoman.

Let me say that first of all in the broader context, also to the Ranking Member's question, that we are satisfied with the text as we have negotiated and look forward to the commission advancing that to the council for approval. We look forward to the council approving it and giving it to the parliament and voting positively on that.

In terms of a law enforcement cooperation, we have added into the new text some ability to facilitate greater cooperation in law enforcement. But as it pertains to U.S. law enforcement, the provisions that would be most important really apply to our Federal law officials.

When somebody gets off an airplane from another country they go through customs and borders. So the information PNR records are evaluated in advance of arrival, as is other information so that if there is additional screening that is required, our customs officials take that into account.

Then the third point, on sea ports, we do look at PNR for people coming in to our ports.

Ms. HAHN. Is it as extensive as—are we connecting the dots as much in that area, do you believe?

Mr. BUSH. PNR as an industry tool is not as well-developed in the sea environment, but we do have the same ability to connect the dots and do run the same pattern-based rules and use the automated targeting system on cruise ships.

Ms. HAHN. I just want to go on record to say, again, my concern will always be on this committee as well as Homeland Security Committee—I mean, on the subcommittee, is that our sea ports, I believe are still an extremely vulnerable entry way into this country, both with cargo and with passengers.

I just want to go on record saying that.

Mr. MEEHAN. Thank you, Ms. Hahn.

The Chairman now recognizes the gentlelady from New York, Ms. Hochul.

Ms. HOCHUL. Thank you, Mr. Chairman, Ranking Member.

My district is on the border of Canada. What standards are in place with respect to airlines that come in from Europe, stop in Toronto and continue to the United States?

We have a different set of standards for Canadian and Mexican-originated flights versus what is considered at the European Union or identical standards.

You can just enlighten me a little bit on that before I ask my next question.

Mr. HEYMAN. We have the same standards and requirements for all of those flights. The secure flight program that the Department of Homeland Security put in place also requires information are provided for all the flights.

So, if a flight were to go to Canada but not to the United States, we would still be able to do the risk assessment for U.S. security.

Ms. HOCHUL. Have any of our other partner nations outside the European Union raised any privacy concerns or any issues or is this it?

Ms. CALLAHAN. With regard to privacy concerns and the use of passenger name records, it has exclusively been a conversation with the European Union.

Mr. HEYMAN. Let me elaborate.

Actually, there are 250 some-odd last points of departure where we require, because of Congressional law, passenger name records to be provided in advance of a flight.

Some of those are in Europe, but the bulk of them are outside of Europe. The European agreement is the only one that we have for that.

Ms. HOCHUL. If we are not successful in negotiating this agreement with the European Union, what is the effect?

The 2007 agreement stays in effect until 2014? Is that how it is?

Okay. So we are not bumping up against a wall just yet. You are just having these negotiations at the stage that we are not under the gun. We are not going to have this program suspended any time soon, correct?

Mr. HEYMAN. That is correct. The Europeans have said that the agreement is provisionally in effect until negotiations are concluded.

Ms. HOCHUL. I know that some have suggested that we suspend the visa waiver program for European countries if we are unable to negotiate, that. Given that about 16 million people come in from Europe to our country, do you think you could handle that additional workload if that would be the case?

Yes. I didn't think so.

[Laughter.]

Ms. HOCHUL. What would be the effect?

Would that compromise the program we have in place with the additional workload? What is your opinion?

Mr. HEYMAN. Actually, first of all it would be terrific if we were to expand our trade-travel opportunity for people who come to the United States. I think it would be a good investment in America. So I think it is a positive step in the right direction.

I don't have the technical specifications in terms of our data analysis capabilities. That is why I was looking over to Tom.

But I suspect first of all this would be ramped up over a period of time, and so we would in fact be able to match the increase if there was a need.

But right now, I think we have the capacity for additional expansions. Is that right?

Ms. HOCHUL. I am very pleased with how this program is working. But how often do you get the situation where you do get someone who is innocent or has the same name, who has to go through additional scrutiny.

Are you able to quickly correct those?

I know you talked about the people who can file the FOIA request and they can correct their record. Early stories were not that simple.

I mean people from my district, it took a long time to get themselves off the list just because I have a community—the Yemenites in my community, others were getting more trouble.

Again, I am supporting what you do. I don't want to compromise the heart of your program.

But I just want to make sure—you said you have made progress in having people removed from that list who have the same name, but have no other reason to be tracking them or giving them additional secondary or additional screening.

Ms. CALLAHAN. DHS takes the issue of providing people appropriate redress and opportunities. The traveler redress inquiry program, I mentioned briefly in my oral statement, has really helped to assist to have a Department-wide process.

For example, you may think that you had a problem at the border because it was a passenger name record issue. But indeed it was something unrelated, therefore they transitioned it.

That has shown great improvement in that we do think that is effective in getting innocent people to have appropriate redress.

Ms. HOCHUL. Okay. Thank you very much.

I yield back the balance of my time, Mr. Chairman.

Ms. SPEIER. Mr. Chairman, I would like to request unanimous consent that the gentlewoman from Texas, the Ranking Member on the subcommittee on transportation security, Congresswoman Jackson Lee, be allowed to participate in this hearing.

Mr. MEEHAN. Without objection, so ordered.

The Chairman now recognizes the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. First order of business is to thank you for your courtesies and to acknowledge the importance of this hearing to the Ranking Member and Chairman, and express my interest because of the subcommittee that I have been involved in as it relates to this important issue.

So, I would like to just—well, first of all welcome the witnesses and ask maybe a question that has already been asked.

We know that—though may not be directly related but we know that travel has generated, by a number of culprits, incidences that have harmed the homeland, from the shoe bomber to the trial that is going on in Detroit as we speak that was a traveler and decided to use methods that we had not confronted in the past.

So I guess I am going to ask this general question in helping us in transportation security—since we deal with the international travel as well. Focusing mainly on passenger travel—is the kind of framework that we see going forward in the 21st Century, and the climate that we are in, and where we are seeing individual actors—I consider terrorism now a franchise.

There is no battalion that shows up at your doorstep, maybe just an individual.

How do we pierce that?

Do we pierce that veil with the human resource intelligence or do we need more armor?

Do we need more armor and intelligence at the gateway? In this instance, I am talking about planes, though I know that trains are in the eye of the storm too. But is it more of a focus on human resource or human intelligence rather?

If I could get that answer from all three of the witnesses, please.

Mr. HEYMAN. Thank you, Congresswoman. That is really one of the most important questions, is: How do we look forward in the 21st Century to securing air travel and travel in general?

The Department of Homeland Security takes this issue very seriously. We have put in place over the last decade, I think, an approach which attempts to achieve exactly what you have set forth.

No. 1, we have to have multiple layers from the authorization of travel visas, ESTAs, Advanced Electronics Travel Authorization. That needs to be scrutinized.

From the decision to book travel, PNR records and the other pre-travel engagement that a traveler makes, we can do scrutiny there.

Checkpoints at the airports is another layer. When a person gets on an aircraft we have security on planes. Then before they get to the United States there is additional scrutiny.

So we have a number of layers of defense that we have put in place to ensure that we prohibit, and prevent, and detect those who seek to do harm from even getting on a plane to begin with. That is with a system that Congress has helped put together through a number of laws and appropriations over the last decade.

I think the PNR system that we have now have been discussing today plays a central role in that.

It allows for us to do not just detection of those who are known or suspected terrorists by going up against the—matching against the watch list that we have, the terrorist database. But allows through certain analysis to detect those who may be unknown to us, but exhibit certain behavior that can allow us to then prevent them from getting on a plane or doing additional screening at a time, so a number of different layers.

Information sharing is critical to that and so that is why we are having the negotiations and having relationships with third parties

and other countries to ensure that we have that information exchanged.

Ms. JACKSON LEE. There is only a little bit more time. Maybe in your answer you would also include whether we are invading a person's privacy on the behavioral aspect, but I think you are talking about utilizing as well.

Ms. CALLAHAN. So, I can take that one up, ma'am.

With regard to information sharing, with regard to screening at the border, I think that we have done—the developments in the past decade have been extraordinary.

But at the same time what has been important is the Department has included privacy protections as they develop these programs. I think that that is crucial for going forward.

Mr. BUSH. Yes, ma'am. I think you hit it on—right away the difference between the intelligence and information sharing and the need for the armor. I think both have to come in.

Obviously with the increasing attempted acts of terror by those not on the watch list really stresses the need for the intelligence information sharing within the Federal Government, but also with our foreign partners.

But once we identified a likely suspect, how can we then detect if they have something on them or attempting to get on a plane are two equally challenging areas.

Ms. JACKSON LEE. Thank you.

I yield back.

Mr. MEEHAN. Thank you, Ms. Jackson Lee.

I have a couple of follow-up questions. I will certainly open the courtesy to the other Members of the committee who are here today if they would so like.

But may I ask—well first, I want to follow up with what the gentlelady just said. The two important points, that aviation continues to be an area that is targeted to be sure, and the, you know, the concern we have that individuals will try to exploit that.

But, Ms. Callahan, there has already been a great deal of work that has been done in terms of protecting the privacy of information as we move along. This has been part of the DHS mission. We constantly move forward and seek information.

Oftentimes there is not enough attention paid to what we are doing with that information behind us or assuring that there are protections that are done. I think simply the fact that we are having this hearing identifies Congress' appreciation and desire to participate in this.

As I have researched this and looked at this particular issue, there is something called fair information practice principles and other standards that are in place.

Could you explain to us just what they are and how they help to secure the privacy of individuals both within the United States and outside?

Ms. CALLAHAN. Absolutely.

Absolutely, sir, thank you for that question.

The fair information practice principles are core elements of essentially all privacy laws throughout the world that has privacy laws. A basis of it was originally in the Privacy Act of 1974 which was the first National privacy act in the world.

It is also embedded in the OECD Privacy Principles of 1980 which, of course, is the genesis for both the European privacy law as well as the U.S. law.

The Department of Homeland Security embeds the Fair Information Practice Principles, or the FIPPs within each of its activities associated with programs, technologies, systems, and information sharing. That is what my office does.

The Fair Information Practice Principles include transparency, individual participation, purpose limitation, data security, data usage, access auditing and accountability, and redress.

All of those elements are important cornerstones that I tried to address in my oral testimony to explain how PNR is an example of the Fair Information Practice Principles as implemented.

Mr. MEEHAN. Can you give me an example of one of those and how that serves as a check against the abuse of that information?

Ms. CALLAHAN. Well, one of the points that the Ranking Member had said is wanting to be more clear with what we are doing with information.

We have tried to be very transparent with the passenger name records and what we are doing. I look forward to any other opportunities to discuss it in order to do that.

In addition, for example, the purpose limitation, to make sure that we are using passenger name records for terrorism, transnational serious crimes, as well as to identify individuals with whom we may want to have more border security to not have the potential for mission creep for example.

Those are important elements and that is what my three audits that are available in my website all show that we are indeed adhering to the principles that we said we would when we first set up the program. That is a very important part of the Department.

Mr. MEEHAN. One of the principles you identified was redress which allows an individual to challenge the information that is in there. So there is already, as I understand it under the FOIA, of the ability to obtain your own record and to request that there be changes in inaccurate information with respect to your own record.

Did I understand your testimony correctly that there are some 220,000 foreign requests for FOIA?

Ms. CALLAHAN. Let me clarify. Two hundred and twenty thousand FOIA requests that we received from across the world. Of those we received them from 100-plus countries. But in terms of proportion, I can't tell you the proportion whether they are U.S. citizens here in the United States or also overseas.

Mr. MEEHAN. Oh, but that may include U.S. citizens——

Ms. CALLAHAN. It absolutely does include U.S. citizens.

Mr. MEEHAN. But that would be an important thing. I mean, I don't know that I need you to do this just to do it.

But if there is some way to analyze and identify the breakdown that may be relevant to this question, I would like to know if we are seeing a disproportionate amount of requests from foreign nations.

Ms. CALLAHAN. The majority—about 75 percent of the FOIAs that we receive actually go to citizenship and immigration services associated with alien files, with their immigration records to obtain information about that.

Mr. MEEHAN. That may be relevant to their interest in trying to obtain citizenship or other kinds of benefits.

Ms. CALLAHAN. Exactly.

So I can tell you that that is where the majority of the requests come in. But a lot of those people are also naturalized U.S. citizens or legal permanent residents who are seeking their information.

With regard to PNR, I can give you the breakdown for the 69——

Mr. MEEHAN. I just wanted to see if there was a dramatic imbalance for some particular reason.

This last issue——

Ms. CALLAHAN. There doesn't appear to be——

Mr. MEEHAN. But the redress is sufficient. Or I am seeing some concerns that somehow we should open up the courts for further redress in some—what is your position on that?

Ms. CALLAHAN. As I mentioned earlier, the traveler redress inquiry program that DHS has stood up is designed to be a one-stop shop available on-line to multiple individuals regardless of where you are and for free.

I think it is a very efficient and effective process that 140,000 people have already sought redress through.

With that said, the European standard thinks that a judicial redress opportunity would be one that would be better.

If you go through a TRIP, you actually have the opportunity to go to court to challenge it. So therefore, I think that to request judicial redress, particularly with the use of PNR, it is probably not necessary because it already is available in the U.S. system.

Mr. MEEHAN. Right.

Well, thank you. My time has expired.

I will now turn it over to the Ranking Member for any further questions she may have.

Ms. SPEIER. Thank you, Mr. Chairman.

Along those same lines, Ms. Callahan, of the 69 requests that you have had for redress, could you make the specifics of those cases or a handful of those cases available to the Chairman and the committee so that we can see what it is they are objecting—I would like to get a better sense of what the concern is.

Because based on the 19 fields that you just listed—and I am a privacy queen. I mean, I have spent a good part of my career trying to protect people's privacy.

I am not seeing where there is a potential even for abuse based on the information that is being shared.

So, either you are taking this information and using it with other information you get from other sources, which if you are you need to explain that to us, or I am missing something.

Ms. CALLAHAN. If I could clarify what the 69 requests were.

They are the request for FOIAs, so just to receive access to their information. Of those 69 FOIA requests—so we don't know if there is a redress problem with it per se.

Of those 69 requests, about half of them come from American citizens who were seeking their own access. About a quarter of them come from the European Union, Canada, and Mexico, and a quarter come from the rest of the world. So it is just an interesting breakdown to see how it evolved.

It originally was more heavily weighted towards Europeans, but now we are getting more from the rest of the world.

With regard to the use and with regard to the access, as Mr. Heyman and Mr. Bush noted, the fields that are being provided are the fields that are being provided to an airline, and therefore they don't inherently have sensitive information in it.

With that said, it is commercial data that the United States is acquiring as part of this Federal border security. So I do think it is important to note that when the U.S. Government acquires commercial information, we need to treat it very carefully.

I think that that may be some of the reservations that people think because it was originally a commercial information, that that is the problem with it.

With that said, the protections that we had put in place, I think, are very robust, very sufficient, and helped to ameliorate that concern, but also help us protect our borders in the ways that Mr. Bush described.

Ms. SPEIER. But do you take that information and overlay it with other information you have within a database you have internally?

Ms. CALLAHAN. We do compare passenger name records with other datasets that Mr. Heyman talked about including ESTA, APIS—which is the Advanced Passenger Information System, the terrorist screening database, and a few other data fields—and criminal records as well. That is all disclosed in all of our public documents.

Ms. SPEIER. A FOIA request by an individual would be able to access that information that you have?

Ms. CALLAHAN. If they asked for their passenger name records, it would not have that because the information is overlaid, compared, and then they go back to their separate databases.

It is not stored in a unique setting. So it is not a Federal record under FOIA.

With that that said they could ask for the information that Customs and Border Protection utilizes in order to make the border decisions. That is a way of having a broader aperture on the FOIA.

Ms. SPEIER. Now, let us go back to the Shahzad case.

He went through a series of screenings, still got on the plane. It was about to leave before he was apprehended.

So where were the failings in the existing system? What kinds of changes have been made to make sure that doesn't happen again?

Mr. BUSH. I think the first improvement, ma'am, was the increased watch list service out of the Terrorism Screening Center.

It had previously taken up to 24 hours to get someone watch-listed. That has now been streamlined and is real-time. So the soonest he would have checked in his name would hit on the watch list and I think it would have stopped there.

The second thing is the time of which PNR is being submitted to the United States has intervals. It is not real-time every time someone books a ticket or makes some changes.

You had asked earlier, I believe—I apologize, if it wasn't you ma'am—the differences between this agreement and the previous ones.

That is an example of an improvement. We are trying to get any change to the PNR in real time. We are trying to explain the value of that to the Europeans.

Ms. SPEIER. So does the European Union object to that?

Mr. BUSH. I don't think they understand it yet to object to it. I think they are still trying to understand does that mean more data being provided, when we were saying if you originally purchased your ticket and you only change it one time, well then we don't need to have continual submissions of the same PNR.

They are trying to understand that. I shouldn't say it is an objection at this point, but I can defer.

Mr. HEYMAN. They are not objecting to it. I think they are just trying to understand it.

It is a new concept, the idea of having real-time data. It is—for data minimization, so it is good for privacy. It is real-time accuracy, so it is good for data security—for National security.

Ms. SPEIER. You know, for those in the European parliament that appear to be objecting to this negotiated agreement, I would argue that they are better served by this agreement than by the agreement that we are operating under, which to your perspective is broader and has less privacy protection.

So I am kind of mystified by their logic. But, I will leave it at that.

I yield back.

Mr. MEEHAN. Mr. Heyman is not taking the bait.

[Laughter.]

Mr. MEEHAN. Ms. Hahn, do you have any follow-up questions?

All right, well, I want to express my deep appreciation. It is a remarkable topic.

I don't think most of America woke up this morning thinking that PNR was the first thing that was on their mind, but a few of us did. It does show the importance. You have identified the key role that this plays.

I also really appreciate the interest of the committee in looking to assure that we are protecting the privacy interests as well. I think that is similarly a mission for this committee.

I thank you for the work that you are doing on both.

Just one following comment. Mr. Bush, we didn't get into the work that you are doing not just with terrorism, but I am impressed by the work that is done with human smuggling and other kinds of things looking at the pattern activity, and do believe that that is an area that we ought to keep working on.

So I want to thank the witnesses for their valuable testimony, and the Members for their questions.

The Members of the committee might have some additional questions for the witnesses, and we will ask that you respond to those in writing. The hearing record will be open for 10 days.

So without objection, the committee stands adjourned.

[Whereupon, at 11:15 a.m., the subcommittee was adjourned.]

○