



Homeland Security

Privacy Office

October 19, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Re: DHS/OS/PRIV 07-90/Hofmann request

Dear Ms. Hofmann:

Pursuant to the order of the court, this is our eleventh partial release to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated October 20, 2006, for DHS records concerning Passenger Name Records (PNR) from May 30, 2006 to the present including:

1. Emails, letters, reports or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes;
2. Emails, letters, statements, memoranda or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the undertakings;
3. Records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used, disclosed to other entities, or combined with information from other sources; and
4. Complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data from EU citizens.

In our December 15, 2006 letter, we advised you that we had determined multiple DHS components or offices may contain records responsive to your request. The DHS Office of the Executive Secretariat (ES), the DHS Office of Policy (PLCY), the DHS Privacy Office (PRIV), the DHS Office of Operations Coordination (OPS), the DHS Office of Intelligence and Analysis (OI&A), the DHS Office of the General Counsel (OGC), the Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP) were queried for records responsive to your request. In our July 27, 2007 letter, we advised you that we expanded our search to include U.S. Immigration and Customs Enforcement (ICE).

Continued searches of the DHS components produced an additional 36 documents, consisting of 235 pages, responsive to your request. I have determined that 5 documents, consisting of 28

pages, are releasable in their entirety; 5 documents, consisting of 20 pages, are releasable in part; and 26 documents, consisting of 187 pages, are withholdable in their entirety. The releasable information is enclosed. The withheld information, which will be noted on the *Vaughn* index when completed, consists of names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7(E) of the FOIA, 5 USC §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E).

Please note that 8 of the documents that are being withheld in their entirety are drafts of remarks that were prepared for Secretary Chertoff's potential use during his visit to the Johns Hopkins University Paul H. Nitze School of Advanced International Studies. While the draft remarks do contain predecisional deliberative information that is responsive to your FOIA request, the final remarks by Secretary Chertoff do not contain any information that would be responsive to your request. However, we are providing a link to the final transcript for your information. The transcript can be accessed at http://www.dhs.gov/xnews/speeches/sp_1178288606838.shtm.

FOIA Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. FOIA Exemption 2(high) protects information the disclosure of which would risk the circumvention of a statute or agency regulation. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information.

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. It applies to facts divulged by a client to his attorney, and encompasses any opinions given by an attorney to his client based upon, and thus reflecting, those facts, as well as communications between attorneys that reflect client-supplied information.

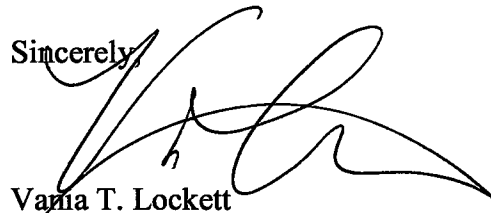
FOIA Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Weighed against the privacy interest of the individuals is the lack of public interest in the release of their personal information and the fact that the release adds no information about agency activities, which is the core purpose of the FOIA.

Finally, FOIA Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Our office continues to process your request. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-90/Hofmann request**. The DHS Privacy Office can be

reached at 703-235-0790 or 1-866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,

A handwritten signature in black ink, appearing to read 'V. Lockett', written over the word 'Sincerely,'.

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 48 pages

Kraninger, Kathleen

From: Kraninger, Kathleen
Sent: Tuesday, August 22, 2006 8:12 AM
To: Agen, Jarrod
Cc: Knocke, William R
Subject: RE: PNR audit

Great. That's what I wanted to make sure you knew about. It is more concrete than saying that the Court found no problems. Wasn't there a statement by the EC that they concurred with the audit? That may be useful as well. Thanks, Kathy

From: Agen, Jarrod
Sent: Tuesday, August 22, 2006 8:10 AM
To: Kraninger, Kathleen
Cc: Knocke, William R
Subject: PNR audit

Kathy – I have this information from DHS Privacy Office on PNR. This fact sheet is most helpful to me in responding to questions on measures we have taken to ensure privacy. Let me know if there is more detail you have on it.

Thanks
Jarrod

http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0724.xml

FACT SHEET

On the Report Concerning Passenger Name Record Information Derived from Flights Between the United States and the European Union

On September 20 and 21, 2005, delegations from the U.S. Department of Homeland Security (DHS) and the European Commission performed the first Joint Review of the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) concerning Passenger Name Record information (PNR) derived from flights between the US and the European Union (EU). Prior to the Joint Review, the DHS Privacy Office conducted an internal review of CBP policies, procedures and technical implementation related to the data covered by the Undertakings. This fact sheet summarizes key points from the Privacy Office report of the internal review.

1. CBP achieved full compliance with the representations in the Undertakings

As of the date of the Joint Review, the Privacy Office finds that CBP is in full compliance with representations made in the Undertakings. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance with the Undertakings. This is a recognizable achievement, particularly because it involves implementation of state-of-the-art technology solutions for use by officers of CBP nation-wide.

2. In cases where implementation took longer than anticipated, CBP has performed remediation at the request of the Privacy Office

CBP undertook responsible measures to address and correct deficiencies that were identified by the Privacy Office prior to the full technical implementation of CBP's IT solutions that comply with the Undertakings.

7/3/2007

3. CBP has put in place an extensive privacy program that includes employee training, procedural and technical controls

CBP has an excellent privacy training program required for all employees with access to PNR data. CBP has also implemented best practices and state-of-the-art technical controls on access, use and disclosures of PNR data to ensure that data is properly filtered and protected from the moment it enters CBP systems.

4. The Privacy Office has had no reports of any deliberate misuse of PNR information

CBP has instituted appropriate technical and procedural controls to regularly monitor access, use and disclosure of PNR data by officers of CBP.

5. Several areas will continue to be monitored by the Privacy Office to ensure future compliance

CBP's data retention schedule has been submitted to the National Archives and Records Administration (NARA) for approval. The Privacy Office will monitor data retention, archiving and disposal for compliance with the Undertakings and the data retention schedule.

Jarrold Agen
Deputy Press Secretary
Department of Homeland Security
(202) 282-9840



**Homeland
Security**

Press Release

October 6, 2006
Contact: (202) 282-8010

STATEMENT BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF ON PASSENGER NAME RECORD AGREEMENT WITH EUROPEAN UNION

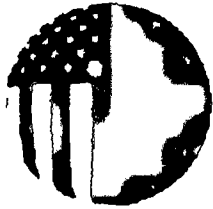
I am pleased to announce the European Union (EU) and Department of Homeland Security (DHS) have reached a final agreement regarding Passenger Name Record (PNR) data which will allow us to make full use of passenger data as needed to protect our borders. This agreement provides the information sharing that I called for in August.

Under the agreement, U.S. Customs and Border Protection will have new flexibility to share PNR data with other counter-terrorism agencies within the U.S. government, carrying out the President's mandate to remove obstacles to counterterrorism information sharing. The new flexibility will apply to agencies within DHS as well as to the Department of Justice, the FBI, and other agencies with counter-terrorism responsibilities: sharing will be allowed for the investigation, analysis, and prevention of terrorism and related crimes. We are pleased that this U.S.-EU agreement promotes our joint goal of combating terrorism while respecting our joint commitment to fundamental rights and freedoms, notably privacy.

I am also encouraged that the agreement will allow the department to receive PNR data earlier, thus increasing our ability to identify potential terrorists. The department will in time obtain access to PNR outside of the 72 hour mark when there is an indication that early access could assist in responding to a specific threat to flights bound for the United States.

The protection of our borders and ability to verify who we are admitting into the United States is a fundamental mission of DHS. I applaud my counterparts at the European Union for agreeing with me on the importance of sharing this passenger data to defend us against terrorism. I want to thank the European Union, EU Vice President Frattini, and my European counterparts for their cooperation and efforts to reach this agreement without impeding travel. I look forward to a continued dialogue with the European Union regarding our data sharing capabilities.

###



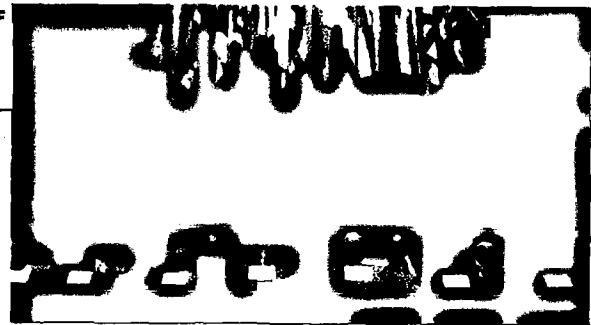
The United States Mission to the European Union

<http://useu.usmission.gov/> Brussels, Belgium

Homeland Security's Chertoff Addresses European Parliament Committee on Data Transfer, Privacy

May 14, 2007

Homeland Security Secretary Michael Chertoff reached out May 14 to members of the European Parliament and the media in Brussels, Belgium, in an effort to allay European concerns about the collection of airline passenger data as part of the U.S. fight against terrorism. In remarks before the Parliament's Civil Liberties (LIBE) committee, he said that access to this information had been crucial to helping prevent terrorist acts.



If such data been available ahead of the September 11 attacks, he noted, U.S. authorities would have been able to find links between 11 of the 19 suicide hijackers.

The U.S. and European Union are currently negotiating a accord on the transfer of passenger name records (PNR), to replace an interim agreement that expires July 31. "It is difficult ... to abandon a tool which at minimal cost to civil liberty, has the tremendous potential to save lives," Chertoff, who appeared with Commission Vice President Franco Frattini and German Interior Minister Wolfgang Schäuble, told the members of parliament. Chertoff also discussed the visa waiver program and mentioned that the U.S. was working on an electronic traveler security system that would involve travelers sending information to U.S. authorities via the internet before beginning their trip.

Below is the unofficial transcript of Secretary Chertoff's remarks before the Civil Liberties committee of the European Parliament in Brussels (Video/Audio):

Secretary Chertoff: Thank you, Mr. Vice Chairman. I appreciate the opportunity and the invitation to be present here in the parliament to address members of the LIBE [Civil Liberties] Committee and other interested observers. I also appreciate not only the remarks of Minister Schäuble and Commissioner Frattini, both of whom are colleagues and friends, but also the cooperation they have demonstrated on behalf of Europe on working with the United States on a whole range of issues where we have common interests and common challenges and with which we want to continue to operate in a

very close partnership to the mutual benefit of all of our people.

This is a particularly good and opportune moment to continue the ongoing discussion we've had on matters that are critical to both the United States and the European Union in terms of security. Earlier this week I had the opportunity to join the G6 Ministers in Venice to discuss some of our shared challenges with respect to preventing acts of terrorism against our countries while making sure that we continue to protect our privacy and our civil liberties. I know this is a commitment each of us shares. None of us wants to forsake our civil liberties in the name of security. On the contrary we seek security that is strong and effective but consistent with the freedoms and values we all cherish as free and democratic nations.

I also want to take the opportunity to emphasize the tremendous cooperation that we in the United States have received from our European colleagues on many fronts in dealing with this challenge of terrorism in the 21st century. We have made a lot of progress as partners and allies, united in the common purpose to defend our nations and citizens against emerging threats in the 21st Century. We have worked together to disrupt terrorist plots both in Europe and the United States. We've enhanced our security across our borders, oceans and skies. We've achieved unprecedented cooperation on a host of international initiatives. From setting standards to sharing information to boosting security at our airports and our seaports. But our work is not done. We still face many challenges.

Some of these challenges are a result of different perspectives that we have on what faces us in terms of the nature of the enemy and the appropriate response. Other challenges reflect the fact that some of the tools and legal and policy approaches that we have at our disposal are not perfectly well suited for the 21st Century adversary that we now face. As my colleague and friend John Reed said a couple of days ago in Venice, we have to consider whether we need to adapt the legal tools and policy tools that have served us in the 20th Century to deal with a different threat that has emerged in the 21st Century.

So the question that we face is how do we move beyond our differences to achieve a new level of cooperation and understanding in areas such as information sharing, privacy and data protection? How do we achieve these goals in a way that respects our fundamental principles but also adapts so that our security goals are well served? In the end, life hangs in the balance. If we do not do our job right, we will see more innocent people perish in wanton acts of violence and terrorism as this decade continues to unfold.

So what I'd like to do is talk a little bit about what I believe are shared fundamental principles and how we approach those principles in dealing with the threat of terrorism that is before us.

I think we have to begin by asking a fundamental question, perhaps the most fundamental question. What are we fighting and why are we fighting it? In other words, what is the nature of the threat we face?

One of the unfortunate side effects of globalization in the 21st Century is the globalization of terror. The same international systems that have bound our societies

together -- air travel, global supply, communications, and financial networks -- are the same systems that terrorists seek to exploit and use against us to cause destruction on a global scale. Today's terrorists fund their operations internationally. They recruit members, they train, they plan and they carry out attacks by exploiting the gaps in the seams in our international systems. The attack of September 11th was a clear illustration of this. The plot was hatched in Central Asia, the recruits came from Saudi Arabia, the training occurred in Afghanistan, the planning occurred here in Europe, and the attack culminated, of course, in the United States with citizens from many countries including many countries represented here lost in the World Trade Center.

Our enemies are determined, they're sophisticated, and they pose a threat not only to the United States but here in Europe, in North Africa, in East Africa, in South Asia, and virtually every place around the globe.

Very recently we've seen clear and tragic evidence of the persistence of this threat in recent attacks in Algeria and Morocco, virtually on the doorstep of Europe. Earlier attacks in Madrid and London. And of course the notable failed attack this past August against transatlantic airliners departing the United Kingdom.

Just this past month a British jury convicted a number of British citizens who had plotted to use fertilizer bombs to attack a shopping mall, a night club, and other targets in London.

There is no doubt about the threat we face. There has been debate about what is an appropriate response to terrorism. Some say that terrorism is just another form of criminal activity to be dealt with in the traditional way we deal with crime. But while law enforcement techniques have some use, I cannot agree that this is the only tool that we can use in order to face this threat. I believe we are at war and that it is essential that we view the threat posed by 21st Century global terrorism in the context of what it means to fight a war.

This is a different kind of war than the war we may have seen in the battlefields in the last century or in earlier centuries, and I will acknowledge it is a war that cannot be won by military might alone. It requires all of the elements of national, and dare I say international power including law enforcement, diplomacy, the use of intelligence, and soft power: the battle for ideas.

The threat that we face is not merely that of a criminal gang or conspiracy. It is an ideological threat. A threat born by ideological extremists who seek to advance a totalitarian vision through the use of terrorism. Al-Qaeda, and the other groups who have affiliated with it, have a world view, a world vision, one that is notably different from that of political terrorists in the past and is distinct from some of the regionally focused terrorist groups that you're familiar with here in Europe.

Again, some have said that al-Qaeda and similar ideological extremist groups are just a variation on the familiar political terrorists that we've seen in earlier places and earlier times, but I would direct you to recent comments from someone who understands well the difference. Peter Clark, who heads counter-terrorism for Scotland Yard in Britain, is a man who fought the Irish Republican Army for more than 30 years. In a speech last month he painstakingly drew a distinction between the terrorists of the IRA with specific

political goals, who did not seek to destroy themselves, and who did not seek to wantonly kill innocent people, and al-Qaeda. He describes al-Qaeda as the reverse of the IRA -- global in origin, reaching ambition with "networks that are large, fluid, mobile and incredibly resilient." It is his judgment, the judgment of an experienced police official, that the threat posed by al-Qaeda and similar ideological groups, is qualitatively different than that which has been faced before here and in the United States.

Of course history teaches us how corrosive ideologies can become when ideas that begin in the early stage seeming merely grandiose or fanciful graduate to having real military power on the world stage.

In the earlier part of the last century the ideologies of communism or fascism did not seem when they first were born as if they constituted a serious threat to world peace, and yet tragically we came to learn that those ideologies left unchecked visited untold devastation and destruction upon the innocent, civilized people of the world.

Therefore, let us talk briefly about what is the goal of the Islamist extremist groups that are behind the terrorist acts that we've seen here in Europe and in the United States. They do not seek merely political revolution in their own countries. They seek the ultimate domination in many countries. Their goal is a totalitarian, theocratic empire, a religious empire, to be achieved by waging perpetual war on soldiers and civilians alike, up to and including the use of weapons of mass destruction.

Some may say this intent is grandiose, it cannot be achieved. I disagree. Extremists such as those in al-Qaeda, the Taliban and other groups from North Africa to Iraq to South Asia to East Africa, are fighting for and now beginning to achieve control of parcels of territory in which they can train, assemble their own advanced weaponry and impose their own vision of repressive law dominating local life and exterminating local freedom.

And of course there's no doubt that the consequences that these extremists can visit upon civilized people compares with the worst we've experienced in wars. The September 11th attacks were the most devastating single blow ever visited upon the United States by foreign enemies, and the plot last summer to blow up multiple transatlantic airliners in Britain had it succeeded would have not only caused the loss of thousands of lives, but would have devastated the international aviation system and really caused a rupture in the ability to travel between this continent and the United States.

Simply put, our foes have made no secret of the fact that they intend to make war, they are building the capability to prosecute war, and they have begun to reveal to us what would be the horrific consequences should they be successful in their efforts at war.

So how do we fight this terrorist network? We fight it by developing a network of our own. It is the network of free people and civilized people who believe in the rule of law and democracy and freedom even for those who disagree with ideas. That means as such a group of partners we must build a unified set of capabilities that allows us to prevent terrorist infiltration, strengthen our borders without making them difficult for innocent people to cross, increase the level of document security, and share information and intelligence to pinpoint threats.

In some ways intelligence is what I would describe as the 21st Century version of radar. In the last century when we feared an attack with bombs we used radar to detect enemy aircraft that might be coming into the United States or into Europe. But that is of no avail in dealing with terrorists. Terrorists come in under the cover of innocence. They cannot be detected by mechanical radar. They can only be detected by the use, analysis and sharing of intelligence that allows us to separate those who are a threat from those who are innocent.

Now let me speak specifically about one way in which we have used intelligence, which I know is of concern to the members of this committee and to this parliament. That is the use of the Passenger Name Records System.

We have built the system to analyze air traveler information combined with other intelligence as part of our method of building a layer of defenses for the United States. This, of course, has been the subject of much serious discussion with the European Union. I think as we go forward to continue and complete these discussions we have the opportunity to take a fresh look at the issue of sharing this information which in many ways reflects a larger issue -- how are we going to develop a long-term framework to share information that allows us to protect all of our citizens against these very dangerous threats?

It is my belief that we have fundamental principles in common which will give us a firm edifice on which we can build sharing arrangements -- one that respects some differences in the institutional arrangements in our various countries, but that ultimately reflects the shared values we all have in liberty and privacy.

As you know, passenger name record information is that which is collected by the travel industry or the airlines when a person makes an airline reservation. It's basic information. It's nothing that's particularly confidential by its very nature. It's things like your name, passport number, frequent flyer number, credit card information and contact information like telephone and address.

What we do is we take this information and we run it against lists of known and suspected terrorists. We use it to analyze links that may arise or connections that may arise between travelers and others who are known to be terrorists so that we can identify those of the 80 million air passengers who come to the United States every year who we need to take a closer look at.

It is the ability to use this information to identify hidden connections that makes it so valuable as a tool to keep out dangerous people.

What I thought I would do in my opportunity to speak to you today is to talk very concretely about how it is we have benefited from the use of this information. We are not merely collecting this for the idle purpose of having a large database of personal data. We are collecting it because time and again it is proving to us that it will enable us to keep dangerous people outside the United States.

We will be furnishing you with a letter at the close of this session that will lay out in greater detail some of our successes using this kind of information, but let me mention just a couple,

In June 2003 using this kind of passenger data and other information one of our inspectors at Chicago's O'Hare International Airport identified an individual traveler coming in not from Europe but from the Middle East. Based on the information shown through this analysis, the inspector pulled aside this individual and conducted an interview. At the close of the interview the inspector concluded that this individual should not be admitted into the United States.

We encountered this individual two years later, or rather we encountered his fingerprints, because in 2005 we found his fingerprints on the steering wheel of a truck which had been used as a vehicle-born improvised explosive device, had been detonated in Iraq and had killed 132 people.

Quite simply, we kept a man out of the United States who later proved to be a suicide bomber. And while I cannot tell you he would have detonated a bomb in Chicago or elsewhere in the United States, I can tell you I would not like to take that chance.

In September 2006 our inspectors at Minneapolis-St. Paul airport used this kind of information -- passenger name record information -- to select a high risk passenger for further examination. When we did so, we asked him questions and we began to examine his baggage. What did we find? We found video clips of improvised explosive devices used against U.S. soldiers and vehicles; we found a video on martyrdom; and a manual on how to construct improvised explosive devices.

After we took him into federal custody, additional searches revealed that he had used the internet to gather information on a special weapons facility in Iraq as well as the England-France Tunnel. In December this individual plead guilty to visa fraud. Again, can I guarantee that this person would have detonated a bomb in the United States? No. Would I want to take that chance? No.

Finally, let me talk about a bit of history, or rather what might have been. Some have gone back and looked at the hijackers who came in on September 11th, or before September 11th to carry out the attacks on September 11th. They've asked the question whether the kind of analysis we are now doing would have allowed us to prevent that plot from being carried out. So let me tell you what would have happened had we had this tool back in 2001.

First of all, two of the hijackers who appeared on a U.S. watch list would have been identified when they bought their tickets. Three of the other hijackers used the same addresses as the two who we had on the watch list, so we would have been able to identify three additional hijackers. One of them, by the way, was Mohammed Attah. A sixth hijacker used the same frequent flyer number as one of the other hijackers, so we would have identified him as well. Finally, five other hijackers used the same phone number as Mohammed Attah, so we would have identified those five. With three simple analytic moves using this kind of data we would have identified 11 of the 19 hijackers and stopped them from coming into the United States.

It is difficult in the face of that clear tragic lesson of history to abandon a tool which at minimal cost of civil liberty has the tremendous potential to save lives, because after all, life is the primary liberty on which all other liberties depend.

Now let me tell you a little bit about what passenger name record information is not, because there's also a certain amount of misconception about this. We do not use passenger name record data to profile based on race or ethnicity. To the contrary, this information allows us to focus on relevant behavioral criteria developed from our investigative or intelligence work. PNR data doesn't guarantee that a person who comes in can be identified as a terrorist or not a terrorist, but it does allow our officers to make a more informed assessment to determine who should be questioned further at the border.

Finally, we don't use PNR to label people or create a risk score that stays with the person for the rest of their life. It simply gives us a way of analyzing their behavior in conjunction with other things we know so we can pursue further inquiry when they appear at our airports.

The benefits of this analytic technique are clear, but we also have very strong privacy protections. Our Federal Privacy Act and Freedom of Information Act, among other laws, as well as oversight by Congress, American courts, and the Inspector General, provide a very strong guarantee against misuse of this information. In fact the Privacy Act has criminal and civil penalties against its violation. Under our mixed use policy the Privacy Act guarantees extend to foreign nationals.

Finally, we recognize that every human system, no matter how valuable, has its imperfections. Therefore we want to continue to build our capacity to grant redress to people who claim they are unfairly being treated at our borders. We recently established a program called a Traveler Redress Inquiry Program that allows travelers of any nationality to seek redress if they feel they've been inappropriately selected by our targeting systems. In short, while there are some differences in the way we organize ourselves than the system here, I believe in all fundamentals this valuable tool is being used in a way that is consistent with the fundamental values that underlie both of our civilizations.

Finally, let me speak for a moment about the Visa Waiver Program which I know is a matter of great interest. The President announced last year that he would ask Congress to pass legislation that would enable us to admit additional countries to the Visa Waiver Program by creating some greater flexibility in the standards that we now apply. That legislation is before Congress. We're hopeful Congress will act this session to inaugurate it. And if Congress gives us the authority, we look forward to being more flexible in welcoming additional European countries into the Visa Waiver Program while continuing to work to elevate security standards in a way that is consistently applied to all countries for our mutual benefit.

As we consider these issues, passenger name record issues, or visa waiver issues, I would suggest that there are some philosophical approaches that ought to govern what we do. Instead of beginning with very specific rigid, legalistic rules, we ought to begin with shared principles along the lines that we're developing now with the High Level Contact Group. Open democracies should be able to respect each other's privacy frameworks, especially when we share the same fair information principles. We want to work constructively, we want to be transparent, and of course we don't want to sit in judgment of each other.

I believe a clear and compelling case can be made that sharing PNR and other identity information will be a net gain for privacy and civil liberties. It will help us better understand who actually poses a risk and should receive more targeted scrutiny. It will avoid the need for a blanket approach that either sweeps everybody into the net or descends into crude profiling which is something that we do not want to engage in. By being able to positively confirm a person's identity, by leveraging the tools we are currently constructing, we will be able to create a safer world not only for Americans but for those who come from Europe to travel in the United States and vice versa.

With that spirit I'm confident that with my friends here and others here at the European Union we will be able to negotiate a new arrangement that demonstrates our joint commitment to protecting privacy while meeting security.

The United States and Europe do share the same basic values when it comes to protecting our citizens and upholding our freedoms. We have defended enemies in the past working together; we can confront today's enemies if we continue in the same spirit.

Thank you for hearing me and I look forward to continuing this dialogue.

Copyright © 2006 U.S. Mission to the European Union. All rights reserved.



The United States Mission to the European Union

<http://useu.usmission.gov/> Brussels, Belgium

Homeland Security's Chertoff Discusses Data Privacy, Transfer in Media Roundtable

May 14, 2006



Homeland Security Secretary Michael Chertoff reached out May 14 to members of the European Parliament and the media in Brussels in an effort to allay European concerns about the collection of airline passenger data as part of the U.S. fight against terrorism. In remarks before the Parliament's Civil Liberties committee and during a media roundtable, he said that access to this information had been crucial to helping prevent terrorist acts. If such data been available ahead of the September 11 attacks, he noted, U.S. authorities

would have been able to find links between 11 of the 19 suicide hijackers. The U.S. and European Union are currently negotiating a new accord on the transfer of passenger name records (PNR), to replace an interim agreement that expires July 31.

Below is the unofficial transcript of Secretary Chertoff's media roundtable at the U.S. Mission to the EU:

Michael Chertoff
Secretary of Homeland Security
Press Roundtable
U.S. Mission to the EU
Brussels, Belgium

May 14, 2007

Secretary Chertoff: Of course I've just come from Venice where I was invited to spend some time meeting with the G6 which is the Interior Ministers from six of the countries in the EU -- Italy, Britain, France, Spain, Germany and Poland. That affords a very good opportunity to exchange common concerns with my European colleagues who have similar portfolios.

What I'm here to do in Brussels is to meet with members of the European Parliament. Obviously the issue of exchange of information, particularly passenger information, is a topic of concern. It's very much in the news. We are currently working under an interim arrangement or understanding that enables us to continue to exercise our authorities to obtain some basic passenger information about people entering the U.S. while preserving the privacy elements which are a concern not only to Europeans but to the United States as well.

We're looking for a more long-term resolution of this issue because it's critical to us that we can continue to exercise our legal authority to obtain this information, but we also respect the concern of travelers about the way in which it's used and I think we're confident that we have very similar views on the fundamentals and we simply need to take account of some differences in institutional arrangements and governing structures that we have in the United States as compared with those in the European Union.

I don't know that anyone has previously really addressed the European parliamentarians on this issue. Obviously we negotiate with the Commission, but I certainly think that being transparent and having a conversation with your key parliamentarians is helpful as part of an effort in general to broaden the depth of our relationship and our cooperation dealing with the issue of (inaudible). So that's what I'm here to do.

Question: I was wondering whether you actually need or want a full-fledged EU-U.S. PNR agreement or if you'd be content with agreeing on general new guidelines on data privacy and just apply your own PNR rules.

Secretary Chertoff: Of course we do have rules on privacy and they're rules that are backed up with penalties if we violate the rules. So obviously whatever we do in the first instance will have to be done within the framework of our own law.

The arrangement we currently have is what I would describe as an understanding or a series of reciprocal undertakings. Each side states what it's going to do and then based on the other side's representations we're able to go forward and really assure the airlines that they can comply with our law without running afoul of that of protection laws in Europe. I think that's a perfectly reasonable way to proceed, having that kind of an understanding. I don't think we need a treaty or anything with great formality, but we're certainly happy to have some kind of mutual recognition of each other's points of view and each other's concerns and have a process and a set of practices that we mutually recognize we're going to be following. That's what I would call, to use a lawyer's term, kind of reciprocal unilateral undertakings.

Question: So you continue that, having this deal saying how long you can keep the data and how much data you can use and which agency can access --

Secretary Chertoff: I think the idea would be we would tell the Europeans here's how we're going to share, here's our data retention, and understand that we're going to agree to these things which I think and hope will address European concerns. The Europeans would then undertake in return to assure the airlines they are not going to be sued or in some ways penalized for agreeing to share the information with us, or in fact living up to their obligation to share the information with us. So in that sense we would have an understanding or an agreement between the EU and the U.S. about what each

is going to do, and that reciprocal set of understandings I think gives everybody what they need.

Question: That wouldn't be legally binding.

Secretary Chertoff: It would be binding in the sense that any understandings are. If one side is trying to change the understanding, the other side would obviously be free to revisit its understanding. It's not going to be something you go to court over, but it is what we sometimes call a gentlemen's agreement or a handshake agreement. Something of that sort.

Question: Washington has set out quite clearly what it would like. How do you see the Europeans responding? What do you think they're going to do about it?

Secretary Chertoff: I'm hopeful that we can reach a meeting of the minds on this because I don't think what we're requesting is substantially different from what Europeans do. It's consistently what we've been doing over the last year which I don't think has caused anybody any heartburn.

Our fundamental principle is the same, which is that we want to limit the use of this information for dealing with, keeping out, terrorists or keeping out serious transnational criminals. I don't think there can be an objection to that. We want to be able to share, obviously, within our official government agencies who all agree to abide by the same conditions of protection. I don't see any real objection to that.

Obviously there are going to be some different points of view on the details, but I'm optimistic that our fundamental principles are the same.

At the end of the day, from our standpoint, it begins with the proposition that just as Europeans have a right to know who comes into Europe, we have a right to know who comes into the United States. And to make a determination about who we want to let in and who we want to return based on a reasonable amount of information, nothing that's terribly private, but information that enables us to determine who might be a threat.

So with that fundamental understanding that every country has a right to defend itself -- no one will ever give that up -- we need to find a way to reassure Europeans and the rest of the world that our fundamental privacy principles are compatible with everybody else's, but also to make sure that we don't become so bureaucratic in how we go about protecting privacy that we actually can't do the fundamental job of providing for the security of our own country.

Question: You mentioned that your fundamental principles are the same. As I'm sure you'll enjoy later when you meet with the European Parliament, there are many there, and others civil libertarians in Europe, who would argue there's a complete fundamental disjunction between the American and the European approach. Can you talk a little bit about how you can bridge that gap? There does seem to be a complete cultural clash between how to reconcile security with civil liberty.

Secretary Chertoff: I certainly have spent a lot of time with my counterparts in the Ministries of the Interior, and I don't see any of them in Europe who disagree with the

fundamental importance of security. Anybody who lived through the London bomb plot of last August, which had it not been disrupted would have caused the death of thousands of people, and by the way, would have been the end pretty much of transatlantic air travel as we know it because it would have been a huge impact on the airlines. If several airliners had been blown up over the Atlantic Ocean, I think it would have had a major impact on international travel. Anybody who lived through that understands that if you don't have security and you don't have a way of checking who's getting on planes and who's coming into your country, you are putting people at risk. I'd be amazed if there were people who disagreed with that and who thought that there's no threat and we just should treat the whole issue as if it's not a matter of concern.

In terms of fundamental principles of privacy, again, we have under our laws rules about maintaining information privately, not misusing it. We have a whole Constitution that is devoted to preserving elements of privacy whether it's the privacy of your home or restrictions with respect to other kinds of government activity.

Are there some cultural and historical differences? Sure. I'll give you an example.

In the United States we don't have national identity cards which you're required to carry. My understanding is here in Belgium you have an identity card and if you don't carry it, the police can ask you for it and if you don't have it they can take you to the police station. In the United States that would be considered completely unacceptable as an affront to civil liberties. That doesn't mean the United States is better; it just means that historically we have viewed that as something that is not acceptable. The history and tradition here is different.

The reverse is that there's a concern about data protection here that probably goes beyond what we have in the United States. Here, I'm given to understand, some people believe the way to protect privacy is to stovepipe information. Every agency can only use the information it has and they can't share that information on a regular basis. We're different.

The whole lesson of the 9/11 Commission. The entirety of that investigation over several months and that several hundred page report really boils down to this. You must be able to connect the dots by sharing information about government agencies. Repeating what we had prior to 9/11 which is some of the information is in the FBI, some of the information is in the CIA, they don't talk to each other, and as a consequence people come in and kill 3,000 Americans, that's not acceptable in America. Again, our traditions and our experiences are different.

Does that mean that there's a fundamental disjunction in our value of protecting privacy and liberty? No. Both Europe and the United States are very concerned about protecting people's privacy and liberty. It does mean because of our historical experiences we tend to express the concern by putting a little bit different weight on different elements of privacy in the --

Question: Let me ask you just a follow-up. The Europeans, and [European Commissioner for Justice, Freedom and Security Franco] Frattini himself has expressed frustration at the lack of data sharing across EU member states. I just wonder from your point of view what the deepest frustrations are in terms of information sharing in Europe.

I remember you mentioned several months ago that if someone found an al-Qaeda computer in Afghanistan and wanted to find out if people were planning on entering the U.S., that that would be impossible under the passenger protection. Is that --

Secretary Chertoff: I think under our current passenger -- I'll give you an example. If we -- under the current regime of passenger name record targeting -- if we had been using this prior to 9/11 we could have identified and stopped most, if not all, of the 19 attackers.

For example, two of the hijackers had appeared on the U.S. watch list, so under the system we have now we would have flagged them when they bought their tickets. Then, using this kind of information we would have seen that three of the other hijackers used the same addresses as the two that are on the watch list, including Mohammed Atta. Now we would have known the identity of five of the hijackers. Another hijacker used the same frequent flyer number as one of the ones that was on the watch list. That would have given us a sixth hijacker. Five other hijackers used the same phone number as Mohammed Atta, so taking the chain of steps further, that would have been 11 hijackers.

~~So just going three clicks of the mouse, so to speak, to use a phrase someone else used,~~
we would have had 11 of the 19 hijackers.

I think under a system that prevented us from sharing this information or obtaining this information we wouldn't be able to do that. So that's an example of exactly what we would be giving up if we gave up the authorities that we have now.

Question: Also maybe to understand the [inaudible], to what extent do you consider the EU as an transit point for terrorism going towards the U.S.?

Secretary Chertoff: I'm sorry, I'm not sure I quite caught that.

Question: To what extent do you consider the EU, what's happening into the EU, to EU countries, as a potential terrorism threat towards the U.S.?

Secretary Chertoff: Obviously we look at, there was a bombing in London in July 2005. There was a bombing in Madrid a couple of years ago. There was the London airline plot which was frustrated last August. There were bombings in North Africa recently, which is on the doorstep of Europe. Obviously we have to be concerned about whether there are terrorists who would either originate out of home-grown cells in Europe or might transit into Europe and come into the United States. Because we have a visa waiver program we don't interview citizens of European countries who come in. Therefore that's one level of protection we've given up. ~~So we do obviously have a concern about whether people~~
might exploit that visa waiver program in order to come into the United States. I think it's a concern Europeans share as they look at the problem within their own countries and within the Schengen area about people who might become exploited and might exploit the freedom of movement in order to commit acts of terror.

Obviously the vast majority of the Europeans who are coming to the U.S. are perfectly innocent and we encourage them to come. But so as not to spoil it for the innocent people, we have to make sure that dangerous people don't take advantage.

Question: Can you qualify this concern or this level of concern you see from people traveling from the EU to the U.S.?

Secretary Chertoff: I don't think I can give you a scale of one to ten. I think that we, the observation of the terrorist attacks in Europe, if you listen to what Peter Clarke, the chief counter-terrorism police official in Britain has said, he's talked about the concern of a significant number of plots that they're following in Britain, and a significant number of individuals in Britain who they believe are involved in terrorist activity. I'm sure there are comparable types of threats inside other countries in Europe. You just have to open up your newspaper to see from time to time the arrests that are made by authorities.

To the extent these are people who are nationals of European countries and are under the visa waiver structure, we need to make sure they're not taking advantage of the lack of a visa requirement to come into the United States.

Question: On that point, that visa [inaudible] scheme, there were some reports a couple of weeks ago that the U.S. might consider applying restrictions to certain citizens of EU member states over concerns that they would exploit the visa waiver program. One of the things that was mentioned was [inaudible] for example.

Secretary Chertoff: That was false.

Question: Do you have any other plans tailored to --

Secretary Chertoff: No, we don't plan to tailor the visa waiver program. What we are -- We are interested in people's behavior. That's the way in which we want to deal with identifying threats. If people communicate with terrorists or if their behavior indicates they're a threat, that's what we're focused on.

We're going to treat the visa waiver countries, including any new countries who come in, in identical fashion. There's legislation that we've proposed to Congress, the President talked about late last year, that would do two things. It would loosen up some of the restrictions on admission to the visa waiver program as it relates to visa denials; but at the same time it would require some more information from every traveler, from all countries under the visa waiver program, in Europe and overseas, Europe and in Asia, that would generally elevate the security level.

But the point I want to emphasize is, whatever elevation of standard will apply across the board, equally to everybody. We're not going to pick and choose among some visa waiver countries and favor some and disfavor others. That's out of the question and it hasn't even crossed anybody's mind. Still less are we going to pick and choose among having different requirements for different sub-groups within individual countries.

Question: You mentioned before the cultural and historical differences between Americans and Europeans addressing these issues. From your point of view, from the other side of the ocean, would you see the EU as a whole on this? Or would you identify some countries closer to your views and more willing to come forward on an agreement with you? And would you envisage ultimately the possibility of establishing bilateral deals with some European countries?

Secretary Chertoff: We've been talking to the EU. I'm always loathe to get into the discussion of what the competencies of the EU versus the individual nations is. First of all, because it's a complicated area of law; and secondly, it's not my place to intrude into the politics of the European Union vis-à-vis its individual nations.

We do with the visa waiver program obviously deal on an individual national level because A, our law requires us to; and B, one of the critical concerns on admission to the visa waiver program is the management of your passports. Currently, as I understand it, passports are controlled on a national level within the EU. The EU does not have a common standard and a common control over all the passports. So essentially the EU itself has limitations on its own authority in this area.

But on this Passenger Name Record information we're dealing with the EU now and happy to do so.

Obviously as the European Court decision of -- I believe -- 2006 indicates, this is an area which I believe falls in what they call the third pillar, not the first pillar, so there are some limitations on the EU's authority. We just have to respect the law here as we find it.

Question: On the visa waiver, is there any chance [inaudible] 12 EU countries who are still out of this program to enter at any time soon?

Secretary Chertoff: Sure, there's a chance and we're hopeful we can make progress on that. Right now it requires legislation by Congress and that is, a bill allowing some additional flexibility, that has passed both Houses of Congress. They have not yet passed, not yet joined up together to agree on a final bill. But once Congress acts we will be happy to move forward.

Question: Can you give us any timeframe and tell us maybe which countries would be more prepared than others?

Secretary Chertoff: I can't predict that right now.

Question: Can I ask you, Mr. Secretary, to elaborate on this vast patchwork of regulations in the EU and what kind of problems this creates for the U.S. in terms of information-sharing? The Europeans themselves complain that they can't share information and they have police in one country hold information jealously from...

Secretary Chertoff: I have sympathy for that. That's a problem we wrestle with in our own country. I think the last five years we've made a huge step in the direction of sharing. Not only sharing among federal agencies, but sharing between federal, state and local agencies in the United States. So I understand the deep, ingrained culture that causes people to want to hoard information because that gives them control over operational activity.

I can only tell you this. The day somebody loses their life because you have pieces of information scattered in different agencies and nobody put them together is the day that everybody's conscience is going to be troubled. There's got to be the ability to combat global terrorism by using networking because you can only beat a terror network by

using a law enforcement network. If you can't share information you can't build a network. If you look all over the world in the 21st Century, the way progress is being made is by information-sharing across the board. And if we retard that in the area of law enforcement and security, we're handicapping ourselves in dealing with an enemy that is fully exploiting global networking.

Question: Does that mean if Europe were to introduce a PNR system as projected by [inaudible] into the EU that you would not have objections that data on Americans being passed around the EU [inaudible]?

Secretary Chertoff: I think we should proceed on reciprocity. I think we're prepared to have the same standards apply to us both in terms of security and privacy and we expect the Europeans to obviously put in the same privacy protections that they're asking us to have in place. And frankly, a world in which it's harder for terrorists to move around because at every stage people are identifying them is a safer world.

Question: In the EU-U.S. -- in what you're negotiating now -- what would you want to see different? I understand you feel your hands are sometimes a bit tied by the current agreement.

Secretary Chertoff: Right now I think our current agreement is good. It's an interim agreement. It's not a permanent agreement and there are a couple of issues we have yet to resolve that were not addressed, including the question of how long we retain information. So those are things that will have to be finalized if we're going to put this in place for a longer period of time.

Question: So you basically want more data --

Secretary Chertoff: I don't --

Question: -- more agencies, or --

Secretary Chertoff: I don't think we're looking for more data, I think we're looking to just have the ability to continue to share the way we're sharing, make perhaps some small adjustments to eliminate some bureaucratic issues. Then there are a couple of issues which we did not really address in the interim agreement of which the principal one was the length of data retention. That's an issue which -- It hasn't come up yet because we haven't been doing it for that long -- but at some point that will come up and we have to resolve. We need to be able to keep the data for a long enough period of time to enable us to make effective use of it. Our experience has shown that terrorist plots often unfold over many many years and they have a very long time horizon. Again, we can't afford to blind ourselves to the kinds of connections that would reveal, as I've indicated with respect to the hijackers, that there are terrorists who are linked, who are coming to the United States. Those are a couple of issues were going to have to deal with going forward.

Question: About cooperation, a large number of people in European agencies say the Americans want a large number of information but they don't give us such a large number. Do you agree with that?

Secretary Chertoff: My experience, and I was also at the Department of Justice. We also, sometimes you find pockets of resistance in the United States to sharing. We still haven't overcome all of those barriers. I believe we ought to share and we ought to get the benefit of sharing. Certainly with my own agencies I make it very clear that I expect us to share information, intelligence, with European counterparts. I have to say my experience has been on both sides, that we have done quite a bit of good sharing. For example, our relationship with the French in terms of sharing has always been quite good, at least in my experience. But as I said, there's always cultural resistance. That's something which has to be overcome.

Question: On the SWIFT affair, which I realize is not directly under your remit, what is your personal view as to whether this kind of information taking is justified?

Secretary Chertoff: Because it's not really my area, therefore I'm not that familiar with the details. I can't say much about it. All I can tell you is in general, having been involved in the investigation after the 9/11 hijacking, the ability to track financial information was a critical element of how we developed a full picture of who was behind the 9/11 hijacking. In fact it was the movement of money that was the first tip-off about the connections that led from the 19 hijackers back to some of the people who were ultimately involved in the plot, including Moussaoui, who was convicted and pled guilty for being involved in the conspiracy.

So the general principle of being able to get financial information as a critical element in the war on terror is, I think, I don't think you can argue with that. As to the legal elements, I'm not sufficiently well versed to give you an intelligent answer.

Question: Back to the PNR agreement. I understand that the deadline is July, right? Practically speaking, what happens if you don't have an agreement by then?

Secretary Chertoff: We obviously have a legal right to require the data. I think the concern is the airlines might then be subject to inconsistent obligations. Everybody recognizes that would be a bad thing. My assumption is we're going to reach whatever understandings we need to reach to hold the airlines harmless, make sure they don't get caught between two conflicting rules, and we won't have a problem.

Question: What would the effect be on the EU and the U.S. [inaudible]?

Secretary Chertoff: It strikes me as not a real likelihood that we're going to wind up without some kind of arrangement. So I'm not going to assume, start to hypothesize what would happen if somehow there was a breakdown of what I am confident will happen, which is we will find a way to deal with this issue.

Question: You said you'd need to keep this information for a longer time in order to use it effectively. How long would that be?

Secretary Chertoff: That's exactly the kind of thing I think we probably ought to have a discussion with in private negotiations as opposed to in newspapers.

Question: On what other fields would you be more willing to come forward to meet where European demands are concerned?

Secretary Chertoff: I think if you -- Again, I don't usually like to negotiate through the newspapers. We were able to reach an accommodation on an interim basis with the agreement that we signed last year. I think in many respects the elements of that are reasonable elements. They may need some adjustment, but they're within what, we use the expression within the ball park, or within the soccer stadium of where we want to get.

Again, there was a lot of hand wringing about whether we were going to be able to reach that agreement. We did. Because it's interim and because there are some issues it doesn't address, we have to obviously work out an arrangement going forward, but again, that lays out the kinds of things that we're able to, I think, have a meeting of the minds on in order to satisfy both sides.

Question: People in Brussels including, I think, Commissioner Frattini when I interviewed him last month, was saying that the U.S. -- or some parts of the U.S. administration -- did not actually want a new EU-U.S. PNR deal, but maybe just wanted individual deals with countries or airlines, or just general guidelines. Because it would be easier for you. Is that correct?

Secretary Chertoff: I think we want to get this problem solved. I don't see any reason we can't work out an arrangement with the EU. We did it last year. Obviously there are some issues that have to be addressed. It would be convenient for everybody to do it that way. So that's what we're going to try to do.

Question: Can I ask about home-grown terrorism?

Secretary Chertoff: Yes.

Question: Having traveled around Europe the last few years writing about this, it seems that Islamic radicalism is increasing rather than diminishing here. With the rise of anti-immigrant parties, young Muslim men are being increasingly disenfranchised, joining groups like [inuadible] here and on and on and on.

On the other side of the Atlantic we haven't seen this with the indigenous Muslim population and I just wonder what lessons you think the American experience can bring to bear in Europe as far as home-grown radicalism seems to be one of the biggest root causes.

Secretary Chertoff: Everybody's spending an awful lot of time thinking and talking about this. One of the discussions that we had with the G6 in Venice was this issue of radicalization and recruitment. Although I think at this point the problem in the U.S. is less than we've seen here, I can't tell you that there's no problem. We had a case last week or in the last two weeks involving not native-born Americans but some individuals who came over at a young age as refugees from Eastern Europe, or Southeastern Europe, and they're accused of having been involved in plots, terrorist acts. Obviously there's a case pending so I can't talk about it too much.

But I think we have to look at the following issues. Are there ways that we've been able to assimilate and bring immigrants into the mainstream that have helped us avoid radicalization and recruitment? Is there a relationship between the fact that in the United

States Muslims are generally better educated and more prosperous than the average? Is that a positive factor? What is the psychology of the 21st Century that leads some people to decide they do want to become extremists? How does the internet either promote recruitment or enable people to train themselves or develop a community of extremism that we now have to figure out how to counteract? What is there in the ideology of extremism that is appealing? What does that have to say about some intergenerational conflict, the younger people rebelling against the older generation?

I think there are some common challenges we all face in the West. I think there are some unique challenges for every country because every country has a different experience with migrants. That history and those cultural experiences tend to create different sociological patterns.

We're trying to understand what is the appeal of this ideology, how do people move from becoming ideologically extreme to becoming operational, wanting to kill themselves.

One of the things that struck me was if you looked at some of the people who were convicted in London in the most recent conviction or have been charged in some of the other terrorist acts, it's not just teenagers. Some of them are people who have children. ~~Usually individuals with children or people who are married are considered to be stable~~ and to have outgrown the kind of rebelliousness that sometimes leads you into violent behavior. But apparently it's not necessarily an antidote to this kind of extremism.

This is, I would say, probably strategically the biggest long-term challenge for the West in dealing with this ideological extremism and it also requires us to understand what is going on in other parts of the world where you are seeing that this extremism has at least some appeal to large numbers of people and how do we prevent that from becoming a spawning ground for more terrorist operatives?

Question: Can I ask you a follow-up on that? Do you think that European culture and civil liberties has exacerbated the problem insofar that these groups are allowed to exist. [inaudible] here, for example, is banned in some countries but not in others. In the UK and in some civic courts Sharia can be applied. Do you think the Europeans are being a little bit too liberal with what they're allowing?

Secretary Chertoff: I don't think that civil liberties results in radicalization. It's kind of ironic, because we were talking about the United States being not as civil liberties oriented as Europe. In fact, in this regard, we're probably much more civil liberties oriented. People in Europe talk, for example, about vetting Imams, deciding which Imams can come in based on what they're preaching, or regulating the internet. Under our law, we are very restricted in our ability to have anything to say about what a person preaches or what kind of religious views they espouse, unless they step across the line of literally advocating for violence. But as long as they're just preaching in the abstract, our First Amendment protects religious people from any kind of government intervention.

We couldn't, for example, bar people from wearing religious headdresses in the United States. That would be unconstitutional except in very limited cases like prisons and the military. Whereas here, I gather, in some countries there's debate about doing that.

So that's an area where we actually are much more, probably, civil libertarian oriented. I'm not inclined to think that that's what causes radicalization.

Question: A more general question. The U.S. sees the war on terror from a military perspective but also from an intelligence and police perspective. Would you say that the first is jeopardizing the second in the sense that it is deviating some financial resources to it? ~~Some of the people [inaudible] that were addressed were on the basis of~~ intelligence information, police action, conventional means. Would you say there is a disbalance in these, in the effectiveness of these two approaches?

Secretary Chertoff: No, I actually think they support each other. I think that military action has sometimes enabled us to gather intelligence or has directly disrupted plots ~~and prevented them from being carried out. I think sometimes police activity has~~ gathered valuable intelligence and disrupted plots. I think that in this kind of 21st Century warfare all of the tools are important. Soft power, police power, military power, intelligence power. I think all of these are useful tactics in the strategy. I think it would be a mistake to put any of them aside because I think they all have value.

Question: A few weeks ago the Dutch Minister of Finance, Mr. Bos, said he would ask an ~~inquiry about the use of financial data on Dutch banks established in the U.S.. Is that~~ right? Are those banks obliged to transmit every information they have about their clients?

Secretary Chertoff: I think you're getting out of my area of competence here, so you better find somebody who knows exactly what the rules are for banking. That's one of the few things my department doesn't regulate.

Question: What else did you discuss at the G6 meeting?

Secretary Chertoff: There was a little press conference afterwards. I would say that the principal areas that I was involved in were radicalization, and John Reed, the Home Secretary, did talk about the need to evaluate whether in the 21st Century some of the ~~legal rules that apply to armed warfare and to domestic law enforcement need to be~~ reviewed in light of the rather unique and novel challenges of terrorism which tends to straddle between conventional notions of warfare and conventional notions of police activity. So he raised that as an issue which I think was in the papers. That was essentially what we discussed.

Thanks very much.

Statements by MEPs from the October 11, 2006 Parliamentary Debate on PNR

Sophia in 't Veld, on behalf of the ALDE Group . – Mr President, I have the feeling that I have ended up in the wrong theatre play and I have the wrong script in front of me. The President-in-Office and the Commissioner were talking about the agreement and you completely ignored the side letter from the Department of Homeland Security, which gives an interpretation of the agreement that goes in a completely different direction from what you have just said. So I am afraid that I am unable to share the joy just expressed by the Presidency and the Commission.

I sent a letter – to which the President-in-Office just referred – with a number of questions. I would very much like to get an answer to those questions, preferably during this sitting, or otherwise in writing. For example, you said that there is no change in the number and the nature of the data and there is no change in the level of protection, but how do you then explain the part in the side letter from the Americans that says that, in addition to the purpose of fighting terrorism and related crimes, we will also collect the data to fight infectious disease and other risks? I call that a considerable widening of the scope. The sharing of data has been widened to include agencies which have not all been specified. The Americans now say that they may not apply the agreed data-retention periods even to the data collected under the old agreement.

You said that we have agreed to move to a 'push system': I am sorry, but that is not what I read. I read that the Americans will move to the 'push system' as soon as it is technically feasible. Well, congratulations! That was also part of the old agreement. It has been technically feasible for more than a year and the Americans have simply refused to do it. So how can you present it this way in a press conference?

I would also like to get an answer on the impact on other categories – the precedent that this agreement sets – for example, the bank account details as in the case of SWIFT, and the telecoms records, to which the Americans also have access. Could somebody please reply to that?

I think we should look to the future, because unfortunately we need this agreement. The only other option would have been no agreement, in which case the Member States would not have stood together in solidarity and would have moved ahead and concluded bilateral agreements with the Americans. I think that for the future we need a strong and clear mandate. Such a strong mandate requires the approval of the European Parliament for reasons of democratic legitimacy. That is the only basis on which a new agreement can be concluded. Therefore, I hope that the bridging clause will be adopted as soon as possible. I know that you are our ally at least on that one.

Martine Roure, [rough translation from Google] in the name of group PSE. - Mr. President, Mister the Police chief, I hold before very saying that, for my group, it was urgent to manage a new agreement with the United States. It was indeed not possible to leave the airline companies in the legal blur in which they were since September 30 and under the blow of severe sanctions if they did not transmit the data required. We were to

necessarily find an agreement common to the whole of the Member States of the Union in order to guarantee an equivalent level of protection for each one.

We however are very worried by the facilitation of the transfer of these data. The later transfer of the data to other agencies responsible for the fight against terrorism poses problem if we do not match it suitable guarantees. We request the civil right European from an effective recourse in front of a judge in the event of abuse the use of these data.

We await American authorities which they apply the guarantees of protection that we ask them and who are registered in the declarations of engagement.

We think that it is necessary to also imply the national parliaments. Article 24 of the Treaty provides that the European Union is the contracting part. That does not prevent however the Member States from resorting to a procedure of parliamentary ratification. Thus, during the signature of the legal cooperation agreements with the United States, the Member States, except two of them, made a statement under the terms of which they would be bound by these agreements only after ratification by their Parliaments. Can you assure us that it is the same for the agreement concerning data PNR and, in the affirmative, to say to us to which rate/rhythm will have these ratifications? It is a very precise question for which we would like to receive an answer.

Lastly, the negotiations for the new agreement of 2007 must concentrate on the definition of a total and constraining framework guaranteeing the protection of the safety and the basic rights of the citizens. Let us not fear to repeat it: the national European Parliament and parliaments must be implied. It is in addition necessary to engage a total reflexion on the data protection relating to the European citizens within the framework of the transatlantic relations. Indeed, a recent hearing on the company SWIFT showed us the possible conflicts between the European right and the American right and we must regulate these conflicts: it is of our responsibility.

Brian Crowley, on behalf of the UEN Group. – Mr President, despite the short time available to me, there are three points that I want to raise.

First of all, what further guarantees have the American authorities given with regard to how the data will be used? I know we have the 'push system' and the 'pull system' and so on, but what kind of criteria are laid down for the use of the data?

Secondly, when we hear about actions on a case-by-case basis determining whether a threat exists or if a particular flight may be under threat, how much time do we have to be able to respond to that request for information, and what difficulty will there be in accessing that data? And I mean that from a European perspective as well as a US perspective.

Thirdly, and I suppose most importantly, if we find that some data has been misused, what comeback do we have? What mechanism is in place to ensure that an individual or groups of individuals whose data has been misused can get some kind of comeback from the American authorities?

These are questions which I think all European citizens want to have answered. I agree with the deal, I think it is a good deal in general and better than the previous deal, but there are still requirements for further clarity on it.

Stavros Lambrinidis (PSE). – Mr President, the temporary PNR agreement with the United States continues to treat as non-binding the US unilateral undertakings for the proper use and protection of personal data in the form of a protocol. Why? And how is it possible that the European Council in this case concluded an agreement that seems more flexible on US obligations than even the agreement that a mere private company, SWIFT, was apparently able to negotiate with US authorities for the unacceptable transfer of banking data? SWIFT, for example, has claimed that it can in real time block any US search if it violates the causes for which it has been agreed.

The PNR and SWIFT cases reveal a dangerous political and legal black hole in the protection of our fundamental rights. A third country invoking exclusively reasons of its own national security can apparently impose upon Europe, including directly upon private companies, the level of access to, use, and even protection of, data. This is clearly unacceptable, and, while the whole EU pillar structure has de facto collapsed in these two cases, the Council insists upon denying Parliament the role of an equal partner in fighting terrorism and in protecting fundamental rights. What is now urgently needed is a comprehensive and democratic European approach in cooperation with all our partners on a global level to deal with these issues in the future.

Jean-Marie Cavada (ALDE). (Rough translation from Google) – Mr. President, taking into account the very high number speakers and people present at this debate, I will try not to tire you more. I approve to a great extent the things which have just been known as, on a subject really very serious. I want publicly to thank Mr. Frattini for his effort for information with regard to our commission.

I express myself indeed as a president of the commission of civil freedoms, justice and the interior businesses since my group was already expressed by the mouth of Mrs. Sophie in 'T Veld. I will make two observations, the first touching with the political climate. It seems to to me that, within the framework of the forthcoming negotiations, it will be necessary to work the concept of reciprocity more. I want to speak about the reciprocity of information that we agree to provide to the American services: what can we hope to obtain in the other directions? I am founded with me to ask it bus if it is true that we, Européens, need to be able to land in the United States, in particular for the businesses, one should not under estimating the same need on behalf of the American companies bus much of businesses are done in Europe. We are thus in a relatively balanced position.

The second observation relates to the future. This interim agreement stops in July 2007, it thus will be necessary to prepare the continuation of it, undoubtedly as of the end of the next winter. Taking into account the many questions that the zones of shade of this agreement pose, in particular - what worries me a little - the interpretative letter to which

Sophie in 't Veld referred a few moments ago, is what it seems to you unreasonable, Mister the vice president, to hope to build a kind of compromise from here the next top the United States/Europe, i.e. from here at April 2007? Can one hope to build a transatlantic species of Schengen on the basis of which the United States, on a side, and the European Union, other, could define a framework making it possible to regulate at the same time the problem of the requirements of safety and that of the protection of the citizens? We have right maintaining to a new political base since we will launch out in a few months in the negotiation of a new agreement.

Michael Cashman (PSE). – Mr President, I should like to congratulate the Commissioner. It is not a perfect agreement. When compromises have to be made, agreements are never perfect, but, as Mrs in 't Veld said, it was either an agreement or no agreement. If there was no agreement, we would have had data anarchy and certainly no EU-wide protection for our citizens. I want to associate myself fully with the comments of Mr Cavada, who I believe has taken a really constructive approach.

We need to look at what is happening with PNR and we need to look at what is happening with SWIFT – incidentally, the memorandum of understanding that SWIFT managed to negotiate is a good basis upon which to build any future negotiations. But we can see it also as an opportunity to create this so-called Schengen transatlantic area, because we will come up against these problems time and time again.

However, I should like to say to this House that nothing is being imposed on us. The choice is ours. If we wish to travel to the United States, we will have to abide by conditions set by the United States. If we want to set up a business in the United States, exactly the same principle applies.

We have to negotiate for our common good and this interim agreement is a step in that direction. Congratulations, Commissioner! The easiest thing in the world is to knock something; the hardest is to support it. Well done.

Sarah Ludford (ALDE). – Mr President, the Presidency said that the final outcome is a success, but I say it is a sell-out. We are told that data protection will be in compliance with relevant European standards, but I read in paragraph 3 that the Americans will process data in accordance with applicable US laws, and in paragraph 1 that data will be handed over as required by the Department of Homeland Security.

Then we have the accompanying US side letter which says that they will interpret the agreement as laid down by President Bush's executive decrees on data sharing and access by other agencies. This is a complete assertion of US jurisdiction, so I would like to ask Commissioner Fratini to tell us whether he accepts this accompanying US side letter as an intrinsic part of the agreement.

Paragraph 6 of the agreement says that the Department of Homeland Security is 'deemed' to ensure an adequate level of data protection. Now what on earth does 'deemed' mean? Paragraph 1 says that we are relying on US continued implementation of the undertakings

as interpreted in the light of subsequent events. So we are at the mercy of events to tell us if the US will respect its undertakings! So the Presidency assertion that the earlier undertakings continue to apply is baseless.

The Commission and the Council say that the agreement delivers legal certainty for EU citizens. I agree with this only in one respect: the certainty that their legal rights have been sold down the river, or rather across the pond. This is not theoretical; we have heard all this year on the Temporary Committee on the alleged use of European countries by the CIA for the transport and illegal detention of prisoners, regarding people about whom soft information has been transferred to the United States that has become hard information, leading to people being rendered to places like Syria and tortured for months or years or incarcerated in Guantánamo Bay. This is not theoretical.

Michael CASHMAN (PES, UK) stated that an agreement with the US is essential if the fundamental rights of EU citizens are to be protected. In the absence of an agreement, he pointed out that the US will quite legally ask passengers to sign a data waiver, which would mean that any notion of EU-wide data protection would be absolutely and fundamentally lost. Mr Cashman also stated that an attack on any one EU Member State is an attack on all Member States because of the common values shared by EU citizens.

[] b/c

[] b/c b2

From: [Ahern, Jayson P]
Sent: Friday, June 30, 2006 3:09 PM
To: Baker, Stewart
Subject: Re: PNR

Stewart:

CBP requires each airline to transmit the elements that are already captured within the airline's reservation system. The PNR data collected by each airline varies according to the business needs of the airline; it may also vary for each PNR (e.g. some passengers may provide an email address to the airline, and others may choose not to provide one.) Some European airlines capture large amounts of data, and others capture fewer data elements. In many cases, an airline's PNR contains data that can exceed the 34 elements CBP is entitled to collect per the Undertakings (however, CBP's automated systems delete this data before it can be accessed by users of the system.)

b7E
b2
high
An informal review of the PNR data elements transmitted electronically by 18 EU-based air carriers to CBP indicates, on average, the majority of the carriers are providing approximately [] data elements on a routine basis. The number and specific data elements will vary from airline to airline based upon their business models, but even the carriers capturing the least amount of data in PNR transmit more than eight data elements to CBP.

The [] most frequently seen elements are:

Hope this helps,
Jay

"Baker, Stewart"

Paul"

06/30/2006 10:55

AM

Subject: PNR

Jay,

Can you explain why European airlines are telling the EU that, on average, they only supply 8 data elements to CBP? I've pasted the note we received from a public meeting on FNR below.

Stewart

6. Julia Egerer, Association of European Airlines:

- _ need for legal certainty
- _ single window needed
- _ reduce the types of data requirements
- _ continue dialogue with industry

She also mentioned that on average only 8 data fields are provided to CBP instead of all 34. The LIBE Committee's vice-chairman Stavros Lambrinidis was surprised by this information.

General questions

Given the difficulty of concluding negotiations before September 30, [

]

7

b5

L

7

General questions on further action on the agreement

Now that the ECJ has determined that PNR is transferred for public security and criminal justice reasons and thereby exempt from the provisions of the 1995 Directive,

]

7

b5

L

We've now had experience applying the Undertakings, [

]

b5

7

Your agreement with Canada precludes them from transferring data to third party countries that do not have adequacy findings. [

Questions about particular aspects of proposed EU draft

What is the legal basis for the EU's current draft? [

UK House of Lords Questions:

1. How useful have the Agreement concluded in May 2004, and the current Agreement concluded in October 2006, been in helping the fight against terrorism and other serious cross-border crimes?

ANSWER:

5

7

65

L

J

2. The judgment of the European Court of Justice struck down the legal base of the 2004 Agreement, and the current Agreement had to be concluded in a hurry. The DHS Undertakings which were part of the 2004 Agreement still apply, but are now qualified by a letter from Mr Stewart Baker of the DHS. Would it not be better for the new Agreement to be clear about exactly what its provisions mean?

ANSWER:

7

7

b5

L

J

3. The current Agreement expires at the end of July 2007. Ministers have told us that in negotiations with the German Presidency and the Commission of the European Union the US authorities are likely to press for material changes to the Agreement and Undertakings, and that the negotiations will be challenging. The US will not wish to negotiate with 27 Member States, but would it be helpful if the Governments of a small number of States, including the UK, also took part?

ANSWER:

7

7

b5

L

J

4. Are the US authorities likely to press for more data elements to be made available? How many of those they are currently able to request are in fact being used?

ANSWER:

1

7

65

L

1

5. Would Advance Passenger Information (API) data, such as those obtained from biometric passports, not be sufficient to identify travellers who are on a watch list because suspected of terrorism or other transnational crime?

ANSWER:

1

7

65

L

1

6. The Undertakings do not confer any rights on any person. It seems that the only remedy available to UK citizens who believe that personal data has been misused or the Undertakings breached is to ask the UK Information Commissioner to refer the matter to the DHS Chief Privacy Officer. We wonder whether this is adequate.

ANSWER: *Under U.S. law and DHS policy any traveller, regardless of citizenship or residency, has certain rights regarding the data held about them. Under the Freedom of Information Act they can request that data pertaining to them and held by DHS, including PNR, be released to them.*

Similarly, as a matter of policy, the Department of Homeland Security has extended access to most aspects of our redress system to non-U.S. citizens. Any person, regardless of their citizenship, can request that inaccurate data about them corrected. While the Privacy Act does not require we take these steps, we have done so unilaterally to promote fairness and build trust. In fact, earlier this year, DHS initiated a new, simpler redress mechanism for all travelers – the

Department of Homeland Security Traveler Redress Inquiry Program (DHS-TRIP). DHS TRIP is a one-stop, web-based scheme through which all travelers can seek redress if they feel they have been inappropriately had their travel denied or delayed by any DHS component that interacts with travelers. Similarly, any traveler regardless of citizenship can seek redress through U.S Customs and Border Protection's Customer Satisfaction Unit. The DHS Privacy Officer will also review any complaints from any individual related to the handling of such requests, either directly or indirectly through their home government's data protection official. The PNR Undertakings recognize this regime and allow that any person may complain directly or through their home government data protection official to the DHS Privacy Officer.

The main redress mechanism not extended to British travelers is access to U.S. courts to seek amendment of their record or damages. We recognize this is a difference between U.S. and many European laws, but such changes cannot be made by executive action in the U.S. legal system. The United States also does not allow a traveler to opt-out of the requirement imposed on airlines to make their data available. DHS has provided public notice on its website and in the Federal Register about these practices and most airlines, including British Airways, provide similar notice. Once informed, if an individual chooses to travel to the United States they are offering their consent that their data be collected.

As a matter of practice, only three travelers have sought access to their PNR since 2003. No complaints have been filed since the first PNR agreement went into place in 2004.

7. Would it be lawful under current US legislation to use PNR data for the purpose of data mining or profiling?

ANSWER:

65

8. At present there is a retention period for data of 3.5 years. Mr Baker's letter states that data more than 3.5 years old can be crucial in identifying links among terrorism suspects. The letter also points out that the current Agreement will expire before 3.5 years, and that questions of when to destroy data collected in accordance with the Undertakings "will be addressed as part of future discussions". We have been told that the current US data retention period is 40 years. Is that right? What period would you think appropriate for the new Agreement?

ANSWER:

┌

┐

65

9. The 2004 and 2006 Agreements deal only with provision of data from Europe to the US. Undertaking 45 provides that if the EU implements a passenger identification system which requires carriers to provide access to PNR for passengers flying to or from the EU, DHS will "encourage" US-based airlines to cooperate. We wonder whether it would help the fight against terrorism and other serious crime, and be to the advantage of the US as well as the EU, if the future Agreement dealt with the flow of information both ways?

ANSWER: ┌

65

→

b5

10. When a Joint Review of the working of the Agreement was carried out in September 2005, access by the European data protection authorities to files was restricted on security grounds despite a confidentiality agreement that they were required to sign. In view of such restrictions, do think the Joint Review procedure is adequate to monitor the working of the Agreement? Will a similar provision be incorporated in the new Agreement?

ANSWER:

✓

7

b5

L

J

TACD

11. How will the EU and US ensure that the new PNR agreement, to be signed by July 2007, protects the privacy of air passenger information?

ANSWER: C

b5

7

65

12. Will European travelers be able to count on the new Agreement being consistent with EU data protection principles (safe harbor)?

ANSWER:

65

b5

13. Will the agreement be consistent with the recently disclosed U.S. Automated Targeting System (ATS) program?

ANSWER: *The agreement has always been consistent with the operation of the Automated Targeting System as ATS has been the system of record in which PNR is stored since its inception. The System of Records Notice issued by the Department of Homeland Security this past fall defines the legal operating parameters of the data base. It is not the single description of a traveler's rights or of other protections provided to PNR. To understand how PNR is handled one must review the SORN (published 11/2/06), the ATS Privacy Impact Assessment (published 11/22/06), and other relevant policies including the 2004 Undertakings, Assistant Secretary Stewart Baker's letter of October 2006, DHS access and redress policies including the new DHS Traveler Redress Inquiry Program (DHS-TRIP).*

14. To what extent is Europe planning on replicating the U.S. data-centered approach in its own handling of airline security?

ANSWER: ☐

b5



Homeland Security

September 5, 2006

MEMORANDUM FOR: Stewart Baker
Assistant Secretary for Policy

FROM: Nathan A. Sales
Deputy Assistant Secretary for Policy Development

SUBJECT: ~~C~~ b5 Uses of Passenger Name Records

[b5]

- **Enhanced Link Analysis.** Because of the strict limitations on sharing PNR information outside of CBP, other DHS components are required to make case-by-case requests for PNR information. In addition, the Undertakings currently limit CBP's access to 34 PNR data elements: a carrier's system may include many more data elements, such as frequent flier information, phone numbers, credit card information.

[b2H
b7E
b5]

[
o
o
b2H
b7E
b5
]

- **Earlier and More Frequent Access to Vital Information.** Under today's restrictions, CBP cannot "pull" PNR data from airlines more than four times, nor can it receive more than four "pushes" from airlines, during the 72 hours prior to the departure of a U.S.-bound flight. [

b2H b7E b5]

- **Investigations of Crimes Other than Terrorism.** Under the current Undertakings, DHS is precluded from sharing PNR information for matters that are not related to terrorism or serious "transnational" crimes.

[
b2H
b7E
b5
]

b2H
b7E
b5

- **Streamlined Review Process.** The Undertakings currently commit DHS to an annual joint review. The review held last year, while successful and useful, was a politically charged event that required significant DHS time and resources. The review began with a lengthy independent investigation by the DHS Privacy Office, which 45-page report. Then the European Commission conducted its own review, culminating in a 35-page report that found CBP in substantial compliance with the agreement but also "identified some areas for improvement and monitoring." Replacing the joint review with a more a traditional (and flexible) consultation-and-review clause simultaneously would ensure that meaningful review takes place and would preserve scarce DHS resources for other vital projects.



Homeland Security

September 5, 2006

MEMORANDUM FOR: Stewart Baker
Assistant Secretary for Policy

FROM: Nathan A. Sales
Deputy Assistant Secretary for Policy Development

SUBJECT: [b5] Uses of Passenger Name Records

b5

- **Enhanced Link Analysis.** Because of the strict limitations on sharing PNR information outside of CBP, other DHS components are required to make case-by-case requests for PNR information. In addition, the Undertakings currently limit CBP's access to 34 PNR data elements; a carrier's system may include many more data elements, such as frequent flier information (beyond miles flown and address), phone numbers, credit card information, other individuals traveling on the same reservation,

b5
b2H
b7E

b5
b2H
b7E

- Earlier and More Frequent Access to Vital Information. Under today's restrictions, CBP cannot conduct an automated "pull" of PNR data from airlines more than four times, nor can it receive more than four "pushes" from airlines, during the 72 hours prior to the departure of a U.S.-bound flight. Manual access can occur prior to this 72 hour window and more than four times if a CBP officer obtains authorization from a supervisor. Still greater access can be obtained by working through law enforcement channels.

b5
b2H
b7E

b5
b2H
b7E

- Investigations of Crimes Other than Terrorism. Under the current Undertakings, DHS is precluded from using or sharing PNR information for matters that are not related to terrorism or serious "transnational" crimes.

b5
b2H
b7E

b5
b2H
b7E

Page 3: [4] Deleted

Streamlined Review Process. The Undertakings currently commit DHS to an annual joint review. The review held last year, while successful and useful, was a politically charged event that required significant DHS time and resources. The review began with a lengthy independent investigation by the DHS Privacy Office, which 45-page report. Then the European Commission conducted its own review, culminating in a 35-page report that found CBP in substantial compliance with the agreement but also "identified some areas for improvement and monitoring." Replacing the joint review with a more a traditional (and flexible) consultation-and-review clause simultaneously would ensure that meaningful review takes place and would preserve scarce DHS resources for other vital projects