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

Homeland Security

Privacy Office, Mail Stop 0550

September 1, 2007

Mr. David L. Sobel
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: **DHS/OS/PRIV 07-160/Sobel request**

Dear Mr. Sobel:

This is our fifth partial release to your Freedom of Information Act (FOIA) requests to the Department of Homeland Security (DHS), dated November 7, 2006 and December 6, 2006, requesting DHS records concerning the Automated Targeting System (ATS). These two requests were aggregated to simplify processing. The following is a consolidated list of records requested:

1. All Privacy Impact Assessments prepared for the ATS system or any predecessor system that served the same function but bore a different name.
2. A Memorandum of Understanding executed on or about March 9, 2005 between Customs and Border Protection (CBP) and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.
3. All records, including Privacy Act notices, which discuss or describe the use of personally-identifiable information by the CBP (or its predecessors) for purposes of screening air and sea travelers.
4. All System of Records Notices (SORNs) that discuss or describe targeting, screening, or assigning "risk assessments" of U.S. citizens by CBP or its predecessors.
5. All records that discuss or describe the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.
6. All records that discuss or describe the potential consequences that individuals might experience as a result of the agency's use of the ATS, including but not limited to arrest, physical searches, surveillance, denial of the opportunity to travel, and loss of employment opportunities.
7. All records that discuss or identify the number of individuals who have been arrested as a result of screening by the ATS and the offenses for which they were charged.
8. All complaints received from individuals concerning actions taken by the agency as a result of ATS "risk assessments" or other information contained in the ATS, and the agency's response to those complaints.
9. All records that discuss or describe Section 514 of the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441) and its prohibition against the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists."
10. All records that address any of the following issues:
    a. Whether a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights may appeal such decision and correct erroneous information contained in the ATS;

b. Whether the underlying error rate of the government and private databases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;
c. Whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;
d. Whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;
e. Whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;
f. Whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;
g. Whether the agency has adopted policies establishing effective oversight of the use and operation of the system;
h. Whether there are no specific privacy concerns with the technological architecture of the system;
i. Whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of Title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and
j. Whether appropriate life-cycle estimates, expenditure and program plans exist.

Our August 1,2007 letter summarized our processing of your request to-date. Searches directed to the DHS Office of the Executive Secretariat (ES), DHS Office of Policy (PLCY), DHS Privacy Office (PRIV), the Transportation Security Administration (TSA), and the U.S. Customs and Border Protection (CBP) have thus far produced a combined total of 335 pages. Out of those 335 pages, we provided you with a combined total of 131 pages with certain information withheld pursuant to the FOIA. We have continued to process your request within PRIV, PLCY, the DHS Office of General Counsel (OGC), the DHS Office of the Inspector General (OIG), and CBP.

A search directed to OGC has produced an additional 234 pages of records responsive to your request. Of those 234 pages, we have determined that 44 pages are releasable to you in their entirety, 44 pages are releasable with certain information withheld pursuant to Exemptions 2,5 and 6 of the FOIA, and 146 pages are withheld in their entirety pursuant to Exemption 5 of the FOIA.

A search directed to CBP has produced an additional 11 pages of records responsive to your request. Those 11 pages are enclosed with certain information withheld pursuant to Exemptions 2,5,6, and 7E of the FOIA.

Enclosed are 99 pages with certain information withheld pursuant to Exemptions 2,5,6, and 7E of the FOIA, 5 U.S.C. §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E). Exemption 2 (high) protects information applicable to internal administrative matters to the extent that disclosure would risk circumvention of an agency regulation or statute, impede the effectiveness of an agency's activities, or reveal sensitive information that may put the security and safety of an agency activity or employee at risk. Exemption 2 (low) protects information applicable to internal administrative personnel matters to the extent that the information is of a relatively trivial nature. Exemption 5 exempts from disclosure certain inter- and intra-agency communications protected by deliberative process privilege, attorney work-product privilege, and attorney-client privilege. Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Exemption 7E 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 as it pertains to PRIV, PLCY, OGC, OIG, and CBP. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. This office can be reached at 866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,

for Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 99 pages

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

Homeland Security

2/12/2006

MEMORANDUM FOR: Secretary Michael Chertoff

THROUGH: Al Martinez-Fonts, Assistant Secretary, Private Sector Office

FROM: (b6) Private Sector Office

SUBJECT: Business Travel Coalition's Actions Against ATS

The Business Travel Coalition (BTC) is actively campaigning for the immediate suspension of the Department's Automated Targeting System (ATS). The BTC's primary argument is that the implementation of ATS lacked transparency and public debate. Since December 3, 2006, BTC has filed comments with DHS through the ATS SORN, issued a Press Statement, and asked the worldwide travel industry to sign a letter which is addressed to you, Mr. Secretary.

In the referenced letter, the BTC describes ATS as a "truly monolithic and disturbing data-mining program which allows for the aggregation of personal information on business travelers; forbids travelers from accessing and correcting inaccuracies; provides for the sharing of such information with foreign governments and third parties; and retains travelers' information for 40 years." In this same letter, the BTC urges DHS to "suspend the ATS program immediately; provide substantially more details on the program to us and our elected representatives; and proceed with ATS only through an official rulemaking with a significant public comment period, per requirements of the U.S. Privacy Act of 1974."

To date, the BTC has secured 29 signatory supporters (see attached). (

[b5]

BTC Background: The BTC was formed as an advocacy organization to advance the interests of corporate buyers on government and industry issues. Founded in 1994, the mission of the BTC is to lower the long-term cost structure of business travel by seeking to bring transparency to industry and government policies and practices so that customers can influence issues of strategic importance to them. The BTC publishes *Travelogue* and *BTC Radio* in 80 countries. As Chairman, Kevin Mitchell writes and speaks on airline competition, travel distribution reform and aviation system security. Mitchell has also testified before the U.S. Congress and other governmental bodies, and in 2004, Mitchell testified that the implementation of CAPPS II and Registered Traveler Programs should have transparency and be exposed to public debate.

Please see Attachments and the BTC's website: http://businesstravelcoalition.com/issues/ats.html

Attachment A: BTC's comments on Docket No. DHS–2006–0060 Privacy Act System of Records Notice (dated 12/3/2006)
Attachment B: BTC's Press Statement entitled, "BTC Condemns Massive DHS Screening Program"
Attachment C: BTC's DRAFT Signatory Letter to Secretary Chertoff re: ATS (includes signatories)
Attachment D: Biography of Kevin Mitchell, Chairman, BTC
Attachment E: Testimony of Kevin Mitchell Regarding CAPPS II (dated 4/17/2004)
Attachment F: *Washington Post* Article on the BTC and ATS (dated 12/1/2006)
Attachment G: *Christian Science Monitor* Article on the BTC and ATS (dated 12/6/2006)
Attachment H: *Government Executive* Article on the BTC and ATS (dated 12/11/2006)
Attachment I: DHS Office of Public Affairs' Privacy Impact Assessment Talking Points
Attachment J: DHS Office of Public Affairs' Just the Facts on ATS (dated 12/8/2006)

DEPARTMENT OF HOMELAND SECURITY

Bureau of Customs and Border Protection

Docket No. DHS–2006–0060 Privacy Act System of Records Notice

Automated Targeting System

COMMENTS OF THE BUSINESS TRAVEL COALITION

01▶Introduction

By notice published on November 2, 2006 in the Federal Register, the Department of Homeland Security, U.S. Customs and Border Protection, acknowledged the existence of a system-of-records known as the Automated Targeting System (ATS) that will assign risk assessments to millions of U.S. and non-U.S. travelers who enter and exit the U.S. ATS has apparently been an operational testing mode for 4 years without the knowledge of Congress or the traveling public, American and foreigner alike.

The Business Travel Coalition (BTC) submits these comments to raise serious concerns related to said system-of-records and to urge the Department to **a)** abandon the December 4, 2006 official program implementation date; **b)** provide substantially more details on the program to the public beyond the Privacy Impact Statement released just one week ago; and **c)** per the requirements of the Privacy Act of 1974, replace its current truncated comment process via the Federal Register with an official rulemaking with a significant public comment period.

The Department has stated that the program "will be effective December 4, 2006, unless comments are received that result in a contrary determination." BTC believes that the serious problems raised in its filed comments herein, and those of other individuals and prominent organizations who have filed comments, indisputably require such a "contrary determination."

02▶Fundamental Problem

The Department characterizes ATS, which originated as a cargo screening program 4 years ago, as "one of the most advanced targeting systems in the world." Indeed, this system represents a historically unparalleled, massive data-mining initiative the parameters of which would: **a)** allow for the collection of all manner of personal information on innocent citizens

without their prior consent; **b)** forbid citizens from accessing and correcting inaccuracies in their personal government dossiers; **c)** provide for the sharing of such information with foreign governments and third parties, including prospective employers; and **d)** retain individuals' information for 40 years. Evolving ATS from a publicly-supported cargo screening program begun 4 years ago to a secretively implemented global traveler screening program represents "Exhibit A" in the case against Mission Creep.

03▶Dismissal of the Privacy Act of 1974

The Privacy Act of 1974 was designed and intended by Congress to safeguard the privacy rights of citizens against government intrusion. It was determined by Congress that privacy can be greatly diminished by the collection, use, sharing and storage of personal information by federal agencies. Congress, however, did provide exacting procedures for an agency to exempt a system-of-records for law enforcement purposes.

The Department seeks to exempt ATS from virtually all relevant provisions of the Privacy Act, and in so doing, dismisses the intent of Congress.

Congress made exceedingly clear its intentions regarding exemptions through subsections 5 U.S.C. §§ 552a(j)(2) & (k)(2) of the Privacy Act. Key points from these subsections are summarized below.

Congress:

- identified the kinds of federal agencies that could, by virtue of their law enforcement functions, have systems-of-records exempted from the Privacy Act;
- identified criminals and alleged offenders as those citizens that very narrow information could be compiled on such as arrests and sentencing;
- made explicit that the purpose of the information collection must be for a criminal investigation associated with an identifiable individual;
- required that an agency seeking an exemption must open its decision making process through an official rulemaking with attendant sufficient public comment;
- required an agency to publish a Statement giving the reason why a system-of-records should be exempted from provisions of the Privacy Act; and
- protected the rights of citizens to have access to information collected on them.

The Department does not meet the threshold requirements of the Privacy Act summarized above with respect to justifying exemptions for ATS. The Department cannot possibly posit that millions of travelers are identified or alleged criminals in a criminal investigation. As opposed to a "backdoor" posting to the Federal Register, the Privacy Act requires a transparent, official rulemaking with abundant time for full public participation. Finally, under the Privacy Act, other federal laws and protections trump exemptions for an agency's program with regard to a citizen's right to access to information collected.

The actual language from the subsections of the Privacy Act follows immediately below.

> **(j) General exemptions**
>
> The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (if the system of records is--
>
> (1) maintained by the Central Intelligence Agency; or
>
> (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.
>
> At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.
>
> **(k) Specific exemptions**
>
> The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is--
>
> (1) subject to the provisions of section 552(b)(1) of this title;
>
> (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

04► Lack of Transparency and Public Debate

Given the scope, scale and potential impacts of ATS, and given the public's and U.S. Congress' concerns with CAPPS II, how could the Department have been implementing this traveler screening program in secrecy even as Congress was conducting hearings and

raising concerns in the spring of 2004? How in any material sense does ATS differ from CAPPS II, or Secure Flight? The answer, of course, is that no one outside the Department knows as the details of the program are largely secret; there has been no public debate or Congressional hearings. Moreover, how would ATS fair against the 10 data accuracy and protection criteria Congress established that had to be met before CAPPS II was implemented?

05▶ATS Impacts

Databases are notoriously prone to inaccuracies. No doubt ATS will cause delays for travelers, unwarranted interferences and inconveniences. Missed flights will cause travelers to pay higher last-minute fares to proceed with their travel plans. Business travelers will miss commercial opportunities, and all travelers risk arrest in a foreign country due to an inaccurate dossier.

What's more, many U.S. and foreign-based corporations have employees who are citizens of other countries who travel to and within the U.S., and sometimes work here for extended periods of time. What extra steps would a foreigner be required to take, should his travel be continuously interfered with, and at what expense, to prove that he is not a risk to the U.S. homeland? If one member of a group traveling together is denied the right to travel, would the entire group receive additional screening?

Importantly, Islam is the fastest growing religion among African Americans, many of whom are business travelers. Often conversion to Islam leads to a name change of the kind that could be mistaken for names on various terrorist watch lists. ATS does not even allow the traveler to know he has been rated a threat; such individuals would not have access to timely and complete corrections to their dossiers.

Adding supreme insult to injury is the fact that while U.S. citizens will not be able to access information collected on them, foreign governments and third parties will be able to do so. This is egregious-in-the-extreme and will further erode citizens' confidence and trust in the U.S. government's ability to calibrate, in a thoughtful and balanced way, efforts to frustrate the efforts of those who would seek to do us harm.

According to David Sobel, of the Electronic Frontier Foundation, the U.S. Government, "is preparing to give millions of law-abiding citizens risk assessment scores that will follow them throughout their lives. If that wasn't frightening enough, none of us will have the ability to know our score or to challenge it."

BTC strongly agrees with the Foundation's concern. ATS incorporates criminal arrest records an individual may have and stores them for 40 years. What if a young person commits an offense that would be expunged from his record after a 5-year period? That record could be picked up by ATS and cause a lifetime of nightmarish problems for that citizen. What's more, after many years of tracking such a young person, the government will have a detailed profile on his travel around the world. That is no one's business but the individual's.

06▶Conclusion

The understatement for 2006 would certainly have to be that DHS observers were stunned to learn of the Department's intentions to near-secretly implement such a massively intrusive program behind the backs of Congress and the public. Virtually all aviation security observers had been led to believe the program was for cargo only. Will ATS be applied to all domestic U.S. air travel next on the justification that we have millions of illegal, unregistered aliens living here who could do us harm? How about ferry, bus and rail transportation?

A look at the world's newspapers after the *Associated Press* stories of December 1 ran provides vivid evidence of the harm such a program will cause to tourism and business travel. BTC is afraid that we are on the cusp of transitioning from an international perception of "Fortress America," to something much darker in its implications. One has to wonder what other uses such a vast and rich database could be used for. Certainly, the public's confidence that the Department takes privacy protections, and the laws enacted by Congress seriously, has been all but shattered by these ATS revelations.

BTC urges the Department to take the following immediate steps:

a) abandon the December 4, 2006 ATS implementation;
b) provide substantially more details on the program to the public; and
c) per requirements of the Privacy Act of 1974, proceed with an official rulemaking with a significant public comment period.

In the final analysis, the American people will not stand for their freedoms and liberties being trampled upon, period, full stop. Such reckless governance as represented by the ATS program erodes trust and confidence in government and its credibility as an effective guardian of citizens' interests, including both privacy and security. We live in a democracy wherein the citizenry needs to understand and support government policies if long-term success is to be achieved. When policies go straight to the heart and soul-- our first-principle-belief in personal liberty--then the requirement for transparency, participation and support is at the very highest level, "Code Red," if you will. DHS is currently failing in this most precious of missions.

...

December 3, 2006

Respectfully submitted,

Kevin Mitchell, Chairman
Business Travel Coalition
214 Grouse Lane, Suite 210, Radnor, PA 19087
(610) 341-1850

Founded in 1994, the mission of the Business Travel Coalition is to lower the long-term cost structure of business travel. BTC seeks to bring transparency to industry and government policies and practices so that customers can influence issues of strategic importance to them. BTC recently founded the Full Content Commission (FCC).

Attachment B: Business Travel Coalition's Press Statement on ATS

BTC CONDEMNS MASSIVE DHS SCREENING PROGRAM

Urges Congressional Intervention and Hearings

RADNOR PA., December 3, 2006–The Business Travel Coalition (BTC) today filed comments with the U.S. Department of Homeland Security regarding its proposed Automated Targeting System (ATS), which is slated for official implementation on December 4, 2006. BTC's filing can be downloaded at http://businesstravelcoalition.com/statements/157.html.

By notice published on November 2, 2006 in the Federal Register, the Department of Homeland Security, *U.S. Customs and Border Protection*, acknowledged the existence of a system-of-records known as the ATS that will assign risk assessments to millions of U.S. and non-U.S. travelers who enter and exit the U.S. ATS has apparently been in an operational testing mode for 4 years without the knowledge of Congress or the traveling public.

ATS represents a historically unparalleled, massive data-mining initiative the parameters of which: a) allow for the collection of all manner of personal information on innocent citizens without their prior consent; b) forbid citizens from accessing and correcting inaccuracies in their personal government dossiers; c) provide for the sharing of such information with foreign governments and third parties; and d) retain individuals' information for 40 years.

BTC chairman Kevin Mitchell stated, "Evolving ATS from a publicly-supported cargo screening program begun 4 years ago to a secretively implemented global traveler screening program represents "Exhibit A" in the case against Mission Creep and government abuse of authority. What's more, DHS seeks to exempt ATS from virtually all relevant provisions of the Privacy Act of 1974, and in so doing, dismisses the intent of Congress."

In its DHS filing the Coalition pointed out that according to security experts, databases are notoriously prone to inaccuracies. ATS will no doubt cause delays for innocent travelers, unwarranted interferences and the risk of arrest in a foreign country due to an inaccurate dossier. BTC questions how DHS could have been implementing ATS in secrecy even as Congress was conducting CAPPS II hearings and raising serious concerns in the spring of 2004 about the accuracy and privacy protections of such programs.

DHS observers and privacy watchdog groups were stunned to learn of DHS intentions to near-secretly implement such a massively intrusive program behind the backs of Congress and the public. Adding supreme insult to injury, while U.S. citizens will not be able to access their dossiers, foreign governments and third parties will be able to do so. Will ATS be applied next to all domestic U.S. air travel on the justification that millions of illegal, unregistered aliens living in the U.S. could do us harm, questioned the BTC in its filing. How about ferry, bus and rail transportation?

BTC calls on the relevant Congressional Committee Chairs to schedule hearings on ATS, and urges all Members of Congress to compel DHS to a) abandon its December 4, 2006 ATS implementation; b) provide substantially more details on the program to the public; and c) proceed with ATS only through an official rulemaking with a significant public comment period, per requirements of the Privacy Act.

"Such government recklessness as represented by the ATS program implementation erodes trust and confidence in government and its credibility as an effective guardian of citizens' interests. In a democracy citizens need to understand and support government policies if long-term success is to be achieved. When policies go straight to the first-principle of personal liberty, then the requirement for transparency, participation and support is at the very highest level, 'Code Red,' if you will. DHS is currently failing in this most precious of missions, concluded BTC."

Attachment C: DRAFT Signatory Letter to Secretary Michael Chertoff from the Business Travel Coalition regarding DHS's Automated Targeting System

DRAFT - DRAFT - DRAFT

December [ ], 2006

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Chertoff:

We the undersigned travel industry associations, corporate travel buyers, travel management companies and other industry participants from around the world write to you to express our agreement with the filing on December 3 by the Business Travel Coalition regarding the U.S. Customs and Border Protection's Automated Targeting System (ATS).

We are deeply concerned that such a far reaching and invasive screening of millions of business travelers entering and exiting the U.S. could do significant personal harm to them, and reduce the productivity of the organizations that field business travelers.

ATS is a truly monolithic and disturbing data-mining program which allows for the aggregation of personal information on business travelers; forbids travelers from accessing and correcting inaccuracies; provides for the sharing of such information with foreign governments and third parties; and retains travelers' personal information in a dossier for 40 years.

Of particular worry is that ATS was widely thought to be strictly for cargo screening. It was discovered only recently that data on travelers have been collected for at least four years without the awareness of the U.S. Congress or foreign governments whose citizens are being profiled. What's more, a dossier is being maintained on these travelers without their knowledge or consent.

We Signatories to this letter urge you to suspend the ATS program immediately; provide substantially more details on the program to us and our elected representatives; and proceed with ATS only through an official rulemaking with a significant public comment period, per requirements of the U.S. Privacy Act of 1974.

Sincerely,

Association of Canadian Travel Agencies, Christiane Théberge, Vice-President, Public Affairs
Business Travel Coalition, Kevin Mitchell, Chairman
Guild of Travel Management Companies, Philip H. Carlisle, Chief Executive
Institute of Travel Management, Paul Tilstone, Executive Director
Netherlands Association for Travel Management, W.I.Dayles, Chairman
Travel Management Alliance, LLC, Chris Dane, Executive Director
A Plus Travel Adventures, Dan Lanser, President
Air Liquide USA LLC, Sharon Gammell. Director of Supply Management
Austin Travel, Larry Austin, Chairman & CEO
Aviation Consultants Inc., C. Sam Benson, President
Brown Jordan International, Clay Cooksey, Director of Procurement and Logistics
Butte Travel Service, Henry Woudstra, Manager
Caldwell Travel, Inc., William O. Caldwell, President
Colpitts World Travel, Alan Krensky, President & CEO
Condado Travel, Jose' Targa, President
Executive Travel Associates, Raiford Pierce. Chairman & CEO
Fujitsu Travel, Fujitsu America, Inc., Karin Vonderach, Manager
Liberty Travel, Gil Haroche, President
Linden Travel, Barbara Gallay, President
Lumbermens Merchandising Corp., Kathleen M. Butcosk, VP, Corp. Meetings & Travel
Management Alternatives, Inc., John Heilner, Vice President
MDM Communications, Inc., Michael T. McDonell, President and Chairman
Rich Products Corporation, Jean Covelli. Travel Administrator
Serbin Partnership, Ltd.,Richard Serbin, President
Siemens VDO, Peggy Medeiros, Regional Commodity Manager, NAFTA
The American Experience Foundation, William A. Hanbury, President & CEO
Tower Travel Management, John Smith, President
TUI 4U GmbH, Hartmut Heering, Managing Director
Vision 2000 Travel Group, Tim Anevich, Sales Manager, Meetings & Events
Washington, DC Convention & Tourism Corporation, William A. Hanbury, President & CEO

Attachment D: Biography of Kevin Mitchell, Chairman, Business Travel Coalition

Kevin Mitchell formed the *Business Travel Contractors Corporation* (BTCC) in 1994, as a corporate buying group to advance fundamental reforms to the airline industry distribution system. In 1996, the *Business Travel Coalition* (BTC) was formed as an advocacy organization to advance the interests of corporate buyers on government and industry issues.

As BTC chairman, Mr. Mitchell writes and speaks on airline competition, travel distribution reform and aviation system security, and frequently testifies before Congress and other U.S. and foreign governmental bodies. BTC publishes *Travelogue and BTC Radio* in 80 countries and in advises major organizations on business travel industry issues.

Mitchell was recognized by *Business Travel News* as one of the 25 most influential industry executives for 1994, 1996 and 1997 and was designated Man of the Year in 1998 by the *Commercial Travelers Association* and Person of The Year for 1998 and 1999 by *Travel Agent Magazine*.

Mitchell is a graduate of Saint Joseph's University in Philadelphia where he received a Bachelor's Degree in International Relations. Mitchell worked for CIGNA Corp. for 12 years where as Vice President, Human Resources and Services his responsibilities included: Corporate Travel, Corporate Aviation, Meetings and Incentives, Event Marketing, Communications, Corporate Safety, and The Eagle Lodge Conference Resort.

Mitchell lives in Radnor, PA with his wife Linda and 16 year old son Brandon.

Mitchell may be reached at:
214 Grouse Lane, Suite 210
Radnor, PA 19087
(610) 341-1850

Testimony of

Kevin P. Mitchell

Chairman, Business Travel Coalition

Regarding CAPPS II

Before the U.S. House of Representatives

Transportation and Infrastructure Committee

Subcommittee on Aviation

March 17, 2004

Mr. Chairman and Members of the Committee, thank you for scheduling this hearing regarding the Computer Assisted Passenger Prescreening System (CAPPS II). My name is Kevin Mitchell. I am chairman of the Business Travel Coalition (BTC), which represents the interests of major corporate buyers of commercial air transportation services.

Today, BTC testimony additionally represents the concerns of more than 100 individual travel industry supplier, distributor and technology firms who were Signatories to a letter recently transmitted to this Subcommittee regarding CAPPS II.

BTC testimony also represents the interests of travel industry associations representing hundreds of European Union corporations and travel agencies with aggregate business travel purchases of some $20 billion dollars. These associations service U.S.-based and foreign-based corporations that have employees who are citizens of other countries and who travel to and within the U.S., and sometimes work here for extended periods of time.

The following associations join with BTC in its Statement this morning:

The Institute of Travel Management that represents 1,000 business travel managers, buyers and suppliers in the UK and Ireland;

The Business Travel Association of Germany that represents more than 400 member companies; and

The Guild of Business Travel Agents which accounts for 75% of UK travel management company purchases and represents members such as American Express, Carlson Wagonlit and BTI-UK.

The business traveler, and those organizations that fund business travel activities, would ultimately be burdened with the majority of direct costs of CAPPS II in the forms of taxes, fees and ticket prices. Should the system be plagued with inaccuracies, the cost of disruptions to the conduct of business would also be born by these airlines' best customers. Firms in the travel industry distribution business face unknowable costs at this time to reconfigure their systems in accordance with the requirements of a CAPPS II.

There may be compelling rationale for revamping the current passenger prescreening system that BTC and other interested parties could support. However, as the GAO report and other analyses point out, we do not yet know in a comprehensive way what CAPPS II would be. That is to say we do not understand the privacy and civil liberty tradeoffs required in return for expectations of greater security. Nor do we know about the safeguards, remedies, costs, future program growth and alternatives associated with such an unparalleled program.

Current concerns of aviation system customers and other stakeholders regarding CAPPS II fall into three main categories: **1)** transparency and public policy debate regarding program design, **2)** potential system cost and effectiveness, and **3)** due process and privacy protections. This morning we will offer our assessment of these concerns as well as recommendations that would address them.

TRANSPARENCY AND DEBATE

Some 88% of participants in a recent BTC survey indicated that CAPPS II has been insufficiently debated on a national or international basis. CAPPS II has received relatively little press attention and most U.S. citizens as well as other countries' citizens who travel to and within the U.S. are simply unknowledgeable about the program, its costs and its short and long-term implications. This hearing will serve to elevate awareness and encourage further debate.

By transparency, we do not mean that we want would-be terrorists to understand details such that a system could be outsmarted. Rather, we seek transparency sufficient to know that respected experts in privacy, security, technology, cost accounting and travel industry distribution are centrally involved in developing the best CAPPS II design possible. Furthermore, we seek assurances that Congress would maintain joint accountability with TSA for ongoing program review.

CAPPS II could reach a historic threshold of intrusion on privacy rights that argues for extraordinary oversight. Throughout history, in times of national crisis, the U.S. government often emplaced policies and programs that had the effect of infringing on personal privacy and liberty. Sometimes, as in the case of Japanese Americans during World War II, the cost was dear. Historically, as crises abated, though, policies that infringed upon freedoms were likewise rolled back, or eliminated.

Unlike temporary programs to frustrate past U.S. enemies, CAPPS II, as a response in the U.S. War on Terrorism, is being viewed as permanent in nature; as if the War will be permanent. By definition, if CAPPS II is to be effective, it must be powerful, adaptable and somewhat secretive. By its nature, a government agency that manages a program such as CAPPS II would over time likely seek to expand the program's capabilities and applications while endeavoring to avoid public scrutiny.

For example, if major U.S. infrastructure facilities were successfully attacked via a gasoline tanker, it would be claimed quickly that a version of CAPPS II should be implemented at interstate toll booths. Likewise, if suicide bombers began targeting Amtrak trains, passengers could expect to be color-coded at train stations. Sporting events, political rallies and other venues where freedoms are celebrated could soon follow.

In the final analysis, these steps might indeed be rational and effective ones to take in a continuing War on Terrorism. However, the mere possibility of these unfortunate developments underscores the need for a thorough public policy debate prior to CAPPS II implementation so that all Americans and foreign citizens understand the program and accept the many potentially serious implications.

Importantly, given the program's current scope, permanency and opportunity for expansion, consideration needs to be given to the circumstances under which Congress might be able to determine that the War on Terrorism has been won so that CAPPS II could be rolled back. After all, President Bush states that the War will be won. Alternatively, if less invasive alternatives to CAPPS II become available, a formal mechanism is needed to override natural bureaucratic tendencies to resist change and protect power.

SYSTEM COST AND EFFECTIVENESS

A program with such potentially far reaching consequences such as CAPPS II requires an understanding of the projected total direct and indirect costs over a multi-year time horizon. Knowing the required resources of money, expertise, time and computing capacity would assist in evaluating alternative uses of these resources in other problematic areas of aviation security, such as cargo.

On a more basic level, and beyond the proposed TSA CAPPS II testing phase, we need to know if the program would actually make aviation system security sufficiently better when considering the resources required and the tradeoffs in personal privacy and freedoms.

BTC research since 2001 has demonstrated that business travelers are willing to give up some privacy for security if it can be proven that they would really be more secure. This important burden of proof should be on the government.

Respected international aviation security experts raise the following concerns regarding the potential effectiveness of CAPPS II:

- • **Over Reliance on Technology.** In the view of former El Al airline global security chief Issac Yeffet, the U.S. is currently over reliant on technology, and not very good technology, at airports for carry-on and checked baggage screening, at the expense of developing human expertise. At issue is once CAPPS II is implemented, how would passengers who are color-coded yellow be further processed? As Yeffet states, "Who will interview you? Who will do the investigation? Who will determine who is suspicious when we only train people how to operate x-ray machines and do body searches only when the alarm goes off?"

- • **Value of ID Checks.** Ostensibly, identification systems seek to identify and create two categories of people—potential good guys and potential bad guys. With CAPPS II, the first category (green) contains passengers requiring little screening and the second category (yellow and red) includes passengers that require additional screening measures. However, this kind of system creates a third and dangerous category: Bad guys that do not fit the profile.

  As chief technology officer at Counterpane Internet Security, and identification expert Bruce Schneier states, "Oklahoma City bomber Timothy McVeigh, Washington-area sniper John Allen Muhammed and many of the Sept. 11 terrorists had no previous links to terrorism. The Unabomber taught mathematics at UC Berkeley. Profiling can result in less security by giving certain people an easy way to skirt security."

  Of concern is that a U.S.-based Al-Qaeda sleeper cell could throw 50 members at a CAPPS II until it identified 10 that were color-coded green. Once a person is color-coded green, it follows that he or she would always be categorized as such until and unless something fundamental changes in the person's profile. Such a system could not only provide a false sense of security at considerable economic and

non-economic costs, but it could actually reduce our absolute level of security.

- • **Reduction of Randomness.** TSA states that as a benefit of CAPPS II the current 15% of passengers who are flagged for secondary screening would be reduced to just 2% to 3%. Security experts worldwide consider the possibility of random selection for secondary screening to be a best-practice deterrent vis-à-vis would-be terrorists. Benefits from CAPPS II could be outweighed by the loss of this deterrent.

DUE PROCESS AND PRIVACY PROTECTIONS

There are numerous serious privacy and civil liberty concerns that privacy groups and others have raised that BTC shares. I would like to focus, however, on just those concerns expressed by the Signatories to the letter BTC recently sent to this Committee as well as the concerns of industry associations previously listed.

- • **Secrecy.** TSA is seeking exemptions from the Privacy Act for the CAPPS II program without providing sufficient rationale. So, from the outset, privacy protections would appear to be diluted. Moreover, CAPPS II places the riskiest aspect of the program, the determination of risk and the construction of rules for conducting background checks, into the purview of secretive intelligence and law enforcement programs and databases. This operating platform reinforces suspicion and concern that CAPPS II would be beyond reasonable public review and oversight.

- • **Profile Mistakes.** How would a passenger challenge his risk assessment score and how long would it take to correct inaccuracies in one's profile? It is extremely worrisome to business travelers from around the world that erroneous information in databases might result in their being perpetually flagged for extra screening. With TSA's recently announced policy that a passenger with a bad attitude could have hefty fines levied against him, it would seem that some passengers would be set on a collision course with the U.S. government.

  This issue is particularly important to U.S. and foreign-based corporations that have employees who are citizens of other countries who travel to and within the U.S. and sometimes work here for extended periods of time. What extra steps would a foreigner be required to take, and at what expense, to prove that he is low risk to the U.S. aviation system? If one member of a group traveling together is color-coded yellow or red, would the entire group receive additional screening?

Importantly, Islam is the fastest growing religion among African Americans, many of whom are business travelers. Often conversion to Islam leads to a name change of the kind that could be mistaken for names on various terrorist watch lists. What assurance would there be that such individuals would have access to timely and complete corrections to their records?

TSA is currently in a disagreement with the airlines over who should pay for lost, stolen or damaged luggage. Passengers have claims that are 18 months old, and still unresolved. So, if TSA cannot do right by passengers with a simple compensation issue over luggage, how are passengers to have confidence that they would have better results with correcting inaccuracies in their risk profiles?

- • **The Cost of Mistakes.** Who would pay for false-positive related travel disruptions when a business traveler who consistently scores yellow for unknown and unresolved reasons consequently misses scheduled flights? Who would be responsible for the additive cost of thousands of dollars for walk-up fares required for subsequently scheduled flights? Would a traveler's employer patiently wait 18 months or longer for the traveler to rectify his record with the TSA? The overall cost to a corporation from lost business opportunities could be considerable.

RECOMMENDATIONS

1. **1.** CAPPS II should be strictly authorized for use only in aviation system security.

2. **2.** The process and timeframe for U.S. citizens and foreigners to have their risk profiles corrected needs to be efficient-to-a-fault, and ironclad.

3. **3.** The threshold requirements that Congress wisely placed on the TSA for CAPPS II to be fully funded should be revised to reflect GAO's recently published CAPPS II audit results as well as the ideas and concerns that will come to light from a thorough public policy debate.

4. **4.** An organization such as GAO, answerable only to Congress, should have sufficient national security clearances and attendant authority to monitor all aspects of a CAPPS II including policies, programs and practices of other supporting government agencies and private sector contractors.

5. 5. CAPPS II should be sunseted after 3 to 5 years to enable Congress to carefully evaluate the costs, efficacy and ongoing need for the program and determine if it warrants reauthorization.

Thank you for the opportunity to provide this testimony.

Attachment F: Washington Post Article on ATS, including BTC comments

Massive Terror Screening Draws Outrage

By MICHAEL J. SNIFFEN
The Associated Press
Friday, December 1, 2006; 10:57 PM

WASHINGTON -- A leader of the new Democratic Congress, business travelers and privacy advocates expressed outrage Friday over the unannounced assignment of terrorism risk assessments to American international travelers by a computerized system managed from an unmarked, two-story brick building in Northern Virginia.

Incoming Senate Judiciary Chairman Sen. Patrick Leahy of Vermont pledged greater scrutiny of such government database-mining projects after reading that during the past four years millions of Americans have been evaluated without their knowledge to assess the risks that they are terrorists or criminals.

"Data banks like this are overdue for oversight," said Leahy, who will take over Judiciary in January. "That is going to change in the new Congress."

The Associated Press reported Thursday that Americans and foreigners crossing U.S. borders since 2002 have been assessed by the Homeland Security Department's computerized Automated Targeting System, or ATS.

The travelers are not allowed to see or directly challenge these risk assessments, which the government intends to keep on file for 40 years. Some or all data in the system can be shared with state, local and foreign governments for use in hiring, contracting and licensing decisions. Courts and even some private contractors can obtain some of the data under certain circumstances.

"It is simply incredible that the Bush administration is willing to share this sensitive information with foreign governments and even private employers, while refusing to allow U.S. citizens to see or challenge their own terror scores," Leahy said. This system "highlights the danger of government use of technology to conduct widespread surveillance of our daily lives without proper safeguards for privacy."

The concerns spread beyond Congress.

"I have never seen anything as egregious as this," said Kevin Mitchell, president of the Business Travel Coalition, which advocates for business travelers. It's "evidence of what can happen when there isn't proper oversight and accountability."

By late Friday, the government had received 22 written public comments about its after-the-fact disclosure of the program last month in the Federal Register, a fine-print compendium of federal

rules. All either opposed it outright or objected to the lack of a direct means for people to correct any errors in the database about themselves.

"As a U.S. citizen who spends much time outside the U.S., I can understand the need for good security," wrote one who identified himself as Colin Edmunds. "However, just as I would not participate in a banking/credit card system where I have no recourse to correct or even view my personal data, I cannot accept the same of my government."

Privacy advocates also were alarmed.

"Never before in American history has our government gotten into the business of creating mass 'risk assessment' ratings of its own citizens," said Barry Steinhardt, a lawyer for the American Civil Liberties Union. "We are stunned" the program has been undertaken "with virtually no opportunity for the public to evaluate or comment on it."

The Homeland Security Department says the nation's ability to spot criminals and other security threats "would be critically impaired without access to this data."

And on Friday as the normal daily flow of a million or more people entered the United States by air, sea and land, the ATS program's computers continued their silent scrutiny. At that Virginia building with no sign, the managers of the National Targeting Center allowed an Associated Press photographer to briefly roam their work space.

But he couldn't reveal the building's exact location. None of the dozens of workers under the bright fluorescent lights could be named. Some could not be photographed.

The only clue he might have entered a government building was a montage of photos in the reception area of President Bush's visit to the center. But there was only one guard and a sign-in book.

Inside, red digital clocks on the walls showed the time in Istanbul, Baghdad, Islamabad, Bangkok, Singapore, Tokyo, and Sydney. Although billboard-size video screens on the walls showed multiple cable news shows, there was little noise in the basketball-court-sized main workroom. Each desk had dual computer screens and earphones to hear the video soundtrack. Conferences were held in smaller workrooms divided by glass walls from the windowless main room.

Round the clock, the targeters from Homeland Security's Customs and Border Protection agency analyze information from multiple sources, not just ATS. They compare names to terrorist watch lists and mine the Treasury Enforcement Communications System and other automated systems that bring data about cargo, travelers and commercial workers entering or leaving the 317 U.S. ports, searching for suspicious people and cargo.

Almost every person entering and leaving the United States by air, sea or land is assessed based on ATS' analysis of their travel records and other data, including items such as where they are

from, how they paid for tickets, their motor vehicle records, past one-way travel, seating preference and what kind of meal they ordered.

Government officials could not say whether ATS has apprehended any terrorists. Based on all the information available to them, federal agents turn back about 45 foreign criminals a day at U.S. borders, according to Homeland Security's Customs and Border Protection spokesman Bill Anthony. He could not say how many were spotted by ATS.

Officials described how the system works: applying rules learned from experience with the activities and characteristics of terrorists and criminals to the traveler data. But they would not describe in detail the format in which border agents see the results or in which the databases store the results of the ATS risk assessments.

Acting Assistant Homeland Security Secretary Paul Rosenzweig told reporters Friday they could call it scoring. "It can be reduced to a number," he said, but he clearly preferred the longer description about how the rules are used.

On the Net:

DHS privacy impact statement:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

Associated Press writers Leslie Miller and Beverley Lumpkin contributed to this report.

Attachment G: *Christian Science Monitor* Article on ATS, including BTC comments

from the December 06, 2006 edition - http://www.csmonitor.com/2006/1206/p03s03-ussc.html

Dispute over 'terror scores' for airline travelers: Supporters of the federal system say it's necessary in the terror war. Privacy advocates aren't persuaded.

By Alexandra Marks | Staff writer of The Christian Science Monitor
NEW YORK

Do you know your terror score? Think you don't have one? You may, if you've traveled internationally during the past four years. And that is generating a growing controversy both in the United States and abroad.

The Department of Homeland Security's Customs and Border Protection (CBP) has been quietly assigning travelers, both American and foreign, on international flights a score that's designed to identify high-risk travelers. It's derived from a set of criteria, such as where you're from and whether you have a habit of buying one-way tickets and paying with cash.

CBP officials call the program, which was implemented with little public notice and no congressional approval, a crucial tool to protect the nation. They describe it as a kind of extra electronic border that has the potential to catch terrorists and criminals before they get to an actual border crossing.

"Without a system like this, we would in many ways be blind to potential threats before they arrive," says Jarrod Agen, a DHS spokesman.

But some congressional leaders, privacy advocates, and travel executives believe it's an unparalleled use of data-mining to invade individuals' privacy. Some European leaders also object, claiming the program - called the Automated Targeting System (ATS) - violates a privacy agreement worked out between the US and the European Union.

Opponents are calling on the Department of Homeland Security (DHS) to suspend the program until privacy concerns can be addressed. They say the key problem with ATS is that there's no way for individual to determine that he or she has been flagged. CBP can also share the information it's collected with other government agencies, other governments, and even private contractors. And CBP can keep the data up to 40 years.

"For the first time, a dossier is being built on me and every other innocent citizen that tracks information on them," says Kevin Mitchell, chairman of the Business Travel Coalition in Radnor, Pa. "To add insult to injury ... they say they're keeping the data for 40 years - just in case Kevin Mitchell - whose profile is not threatening at the moment - has some kind of ties to a terrorist organization in the future."

The controversy over ATS erupted after privacy advocates at the Electronic Frontier Foundation (EFF) found an obscure notice about it in the Federal Register last month. In the notice, which is required under the 1974 Privacy Act, DHS says that its data collection system "does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems."

In fact, the data collection system has been in place since the mid-1990s, says CBP spokesman Pat Jones. It was started as a way to help interdict drug shipments and smugglers and was carried out by the Treasury Department. After 9/11, it was enhanced to include potential terrorists, and it was eventually moved to CBP, according to Mr. Jones. "The information that we've got is not invasive. How someone pays for their plane ticket I don't think is an invasion of anyone's privacy," he says. "These issues always involve some kind of a balance."

But privacy advocates contend the issue is far more complex. EFF's lead counsel, David Sobel, notes that prior to the publication of the November notice, the only public mention of ATS said that it was used to target and assess cargo shipments, not people.

"Congress didn't know they were doing this. Even DHS's own inspector general in a report issued this summer didn't realize they were using this to target passengers," he says.

The Transportation Security Administration has been trying to put together a similar data collection system to check air passengers for years, Mr. Sobel and other privacy advocates note. That system, called Secure Flight, has been tabled by DHS until privacy concerns raised by Congress can be addressed.

Mr. Mitchell of the Business Travel Coalition says that while he and others were testifying before Congress about problems with Secure Flight, DHS was quietly collecting almost the same kind of information. And unlike Secure Flight, which is designed to "ping data" and then expunge it, the ATS data is saved in a data bank.

"None of us knew this was going on behind our backs," says Mitchell. "This looks like it was done because [other data-mining systems failed] and Secure Flight's in trouble."

Some congressional leaders, including Sen. Patrick Leahy (D) of Vermont, have pledged to hold hearings on ATS. "Databanks like this are overdue for oversight, and that is going to change in the new Congress," Senator Leahy said in a statement.

For now, DHS is standing by its program and says it has no plans to suspend it for further public scrutiny. "You tell [privacy advocates] when they're able to persuade the bad guys to announce when they're coming into the country, we won't need a system like this," says Jones of CBP.

[**Editor's note:** *The original headline overstated the level of controversy surrounding the terror score program.*]

Full HTML version of this story which may include photos, graphics, and related links

Attachment H: *Government Executive* Article on ATS, including BTC comments

Opposition To DHS Traveler Screening Program Mounts (GovExec/TD)
By Chris Strohm
Government Executive/Technology Daily, December 11, 2006

Opposition to a Homeland Security Department program that screens travelers entering the United States continues to grow and now includes international travel associations that are calling for the program to be suspended.

Outrage has continued to mount since Homeland Security posted a notice on the automated targeting system in the Federal Register last month The notice said the system is used for risk assessments on travelers coming into the country by land, sea and air. Opponents claim that the department kept details of the program hidden from the public for years.

"Privacy is not a niche issue," said Jay Stanley of the American Civil Liberties Union. "It's not a liberal issue; it's not a conservative issue; it's not a special interest."

In the latest twist, international travel associations have signed a letter to Homeland Security Secretary Michael Chertoff. The U.S.-based Business Travel Coalition wrote the letter and has spearheaded a campaign to get organizations to endorse it.

"We are deeply concerned that such a far-reaching and invasive screening of millions of business travelers entering and exiting the U.S. could do significant personal harm to them, and reduce the productivity of the organizations that field business travelers," states the letter, which likely will be sent to Chertoff at the end of this week.

Signatories so far include the Association of Canadian Travel Agencies, Guild of Travel Management Companies, Institute of Travel Management and the Netherlands Association of Travel Management. Three U.S.-based travel organizations also have signed the letter, along with 32 companies, some of which are international.

Kevin Mitchell, chairman of the Business Travel Coalition, said the program appears to closely resemble an airline passenger-screening program known as CAPPS II that was killed due to public and congressional outrage.

"It's a ham-handed, tone-deaf approach to security that sunk CAPPS II and continues to get them in trouble," Mitchell said. "The feeling it leaves people is that if the Department of Homeland Security is going to behave like this in its infant years, what's it going to behave like when it becomes an adult?"

Chertoff offered a strong defense of the program in an interview with CongressDaily. "To hear people are outraged baffles me," he said. "I totally reject that this has been kept secret." He said the program is a critical tool for U.S. border agents to protect the country.

The department, however, has extended the time for public comment until Dec. 29.

Meanwhile, a debate has erupted over whether the program violates a section of the fiscal 2007 Homeland Security appropriations bill that prohibits using funds "to develop or test algorithms assigning risk to passengers" whose names are not on government watch lists.

"Clearly the law prohibits testing or developing computer programs" like the automated targeting system, said House Homeland Security Appropriations Subcommittee ranking Democrat Martin Olav Sabo, D-Minn. But A Homeland Security spokesman said the department believes the prohibition only applies to another traveler screening program called Secure Flight.

Automated Targeting System Talking Points

- To provide expanded notice and transparency to the public, the Department of Homeland Security, U.S. Customs and Border Protection gave notice regarding the Automated Targeting System (ATS) on November 2, 2006 in the Federal Register. This Privacy Impact Assessment provides additional details about the privacy impact associated with this system.
- ATS is not a new program nor does it represent a new collection of information. ATS was initially deployed in the early 1990's to identify cargo that was likely to be entering the United States in violation of U.S. law. Passenger modules were first deployed in the mid 1990's.
    - This assessment is being published now to provide the public with greater visibility into an existing program.
    - ATS is the enforcement screening module associated with the Treasury Enforcement Communications System and was previously covered by the Treasury Enforcement Communications System "System of Records Notice."
- ATS is the primary tool used by CBP to prescreen cargo and travelers destined to the United States. In many cases, it is the United States government's first opportunity to determine whether a good or person presents a risk of terrorism, illegal immigration, trafficking or other criminal activities. Without ATS the United States would be blind to potential threats until they have entered the United States and screening at points of entry would be slower and more cumbersome.
    - ATS treats all passengers and cargo equally. It does not profile on race, ethnicity or arbitrary assumptions.
    - ATS makes an assessment in advance of arrival based on information that DHS would otherwise collected at the point of entry.
    - ATS does not replace human decision making. It provides analysis for use by trained law enforcement officials.
- Significant system safeguards have been put in place to protect the traveling public from the unauthorized disclosure of their personal information. Access to ATS is only given to personnel with a need to access information in the course of completing their official duties and stiff penalties are associated with misuse. Auditing systems have been established to identify unauthorized access and misuse.
- Individuals may seek access to the source information collected in ATS or originating from a government source system pursuant to the FOIA and as a matter of CBP policy.

- With respect to the data that ATS creates, i.e., the risk assessment for an individual, the risk assessment is for official law enforcement use only and is not communicated outside of CBP staff, nor is it subject to access under the Privacy Act. ATS is a system that supports CBP law enforcement activities, as such an individual might not be aware of the reason CBP is engaging in additional scrutiny, nor should he or she as this may compromise the means and methods of how CBP came to require further scrutiny.

- ATS stores data for 40 years because a recently identified transnational criminal or terrorists travel history is frequently relevant to assessing the risk they present and, when appropriate, developing a case against them. To prematurely delete data already collected under existing statutory authority would severely hamper these efforts with minimal impact on an individual's privacy.
    - This retention period for data in ATS reflects the longest underlying retention period for the data in its source records (for example, data from ACS, AMS, and ACE is retained for six years).
    - However, the touchstone for data retention, however, is its relevance and utility. Accordingly, CBP will regularly review the data maintained in ATS to ensure its continued relevance and usefulness. If no longer relevant and useful, CBP will delete the information.

Background on ATS System

- The Automated Targeting System (ATS) is an Intranet-based enforcement and decision support tool that is the cornerstone for all Customs and Border Protection's (CBP) targeting efforts.
    - CBP uses ATS to improve the collection, use, analysis and dissemination of intelligence to target, identify and prevent potential terrorists and terrorist weapons from entering the United States and identify other violations and violators of U.S. law.
    - In this way, ATS allows CBP officers to more effectively and efficiently focus their efforts on cargo shipments and travelers that most warrant further attention.
    - ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data or personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved.
    - Every traveler and shipment processed through ATS is subjected to a real-time rule based evaluation.

- ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities.
    - ATS-Inbound – inbound cargo and conveyances (rail, truck, ship, and air)

- ATS-Outbound – outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) – travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) - private vehicles arriving by land
- ATS - International (ATS-I) - cargo targeting for CBP's collaboration with foreign customs authorities. (in development)
- ATS- -Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)

- Generally, ATS collects and maintains personal information relating to name, risk assessment, and the internal system rules upon which the assessment is based and Passenger Name Record data obtained from commercial carriers.
  - ATS does not collect information directly from individuals. The information used by ATS to build the risk assessment is collected from government data sources and from entities providing data in accordance with U.S. legal requirements or other applicable arrangements (e.g., air carriers providing PNR regarding individual passengers).
  - Relevant data, including personally identifiable information, is necessary for CBP to effectively and efficiently assess the risk and/or threat posed by a person, a conveyance operated by person, or cargo, handled by a person, entering or exiting the country.

Press Office
U.S. Department of Homeland Security

Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

AN ASSOCIATED PRESS STORY CLAIMS THAT THE AUTOMATED TAGERTING SYSTEM (ATS) MAY VIOLATE U.S. LAW: "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT IT IS CLEAR THAT CONGRESS DID NOT INTEND TO LIMIT THE ATS PROGRAM:

- The Aviation and Transportation Security Act of 2001 mandates that each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to Customs an electronic transmission of a passenger manifest and carriers shall make passenger name record information available to the Customs Service.

THE STORY CLAIMS A PROVISION BY CONGRESS PROHIBITS COMPUTERIZED RISK ASSESSMENTS: "But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT WHEN READ IN CONTEXT, IT IS CLEAR THAT THE PROVISION WHICH SOME HAVE SUGGESTED WAS ADDED TO REGULATE ATS (SECTION 514 OF THE DHS APPROPRIATIONS BILL), HAS NOTHING TO DO WITH ATS, NOR WAS IT INTENDED AS A CATCH-ALL PROVISION:

- The various sections of the law cannot be read in isolation. Section 514 is concerned only with aviation security generally and the Secure Flight program administered by TSA in particular. Congress did not intend section 514 to pertain to ATS, a program that has been funded by Congress since the late 1990's and has an entirely different mission from Secure Flight. Secure Flight is intended to screen domestic passengers attempting to board airplanes, while ATS relates to individuals seeking admission to the U.S. at ports of entry.

- ATS has been in existence since the late 1990's. Congress is presumed to be aware of programs in existence when it passes legislation. The fact that Congress makes no mention of ATS undermines the suggestion that it intended to regulate it in any way. Because ATS predates the Secure Flight program, it can be neither a "follow-on" nor "successor" program to Secure Flight, as required by section 514(a).

- Furthermore, the provision prohibits the use of DHS funds "for data or a database that is obtained from or remains under the control of a non-Federal entity," except Passenger Name Record Data obtained from air carriers. This provision only makes sense if it is limited to testing activities for Secure Flight. Otherwise. by this language, Congress would have made illegal any use of non-Federal database material by the federal government, thereby shutting down numerous legitimate programs having nothing to do with aviation security.

THE STORY ALSO CLAIMS THAT THERE HAS BEEN LITTLE NOTICE OF ATS: "ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules. *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT DEPARTMENT OFFICALS HAVE TESTIFIED BEFORE CONGRESS SEVERAL TIMES AND HAVE PROVIDED NUMEROUS STAFF BRIEFINGS AND TOURS OF THE ATS AND THE OPERATIONS AT THE NATIONAL TARGETING CENTER.

- Excerpts from the nearly 20 written testimony about ATS to Congress since May 2003 include:

➢ **DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006):** "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

➢ **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006):** "The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

➢ **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006):** "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher

risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

- **Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004):** "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

- **CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004):** The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

COMMENTS OF REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN-DESIGNATE COMMITTEE ON HOMELAND SECURITY U.S. HOUSE OF REPRESENTATIVES ON DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE PRIVACY ACT SYSTEM OF RECORDS NOTICE FOR THE U.S. CUSTOMS AND BORDER PROTECION AUTOMATED TARGETING SYSTEM

Docket No. DHS-2006-0060, Published Nov. 2, 2006, Extended December 8, 2006

As Chairman-designate of the Homeland Security Committee, I am pleased to submit these comments on the November 2, 2006 Privacy Act System of Notice (SORN) regarding the Automated Targeting System, known as ATS.[1] These comments specifically concern the screening program for passengers, or ATS-P. In the SORN, the Department describes ATS-P as the screening system employed by U.S. Customs and Border Protection (CBP) for "identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law."[2]

I appreciate the Department's decision to extend the comment period to December 29, 2006,[3] as I requested in my letter to the Secretary of December 4, 2006.[4] As explained in that letter, I am concerned that some elements of ATS-P may constitute violations of the privacy and civil liberties of U.S. citizens and lawful permanent residents (LPRs). A detailed staff briefing by CBP officers on December 11, 2006, has resolved some of those concerns, but I believe there remain several aspects of ATS-P itself that require further elaboration or revision. In addition to these comments, I have

---

[1] Department of Homeland Security. Privacy Office, Notice of Privacy Act System of Records, 71 Fed. Reg. 64543-46 (Nov. 2, 2006).
[2] Id. at 64545.
[3] Extension of comment period, 71 Fed. Reg. 71182.
[4] Letter from Rep. Bennie G. Thompson, Ranking Member of the House Homeland Security Committee, to Secretary Michael Chertoff (Dec 4, 2006).

also sent a letter to CBP Commissioner W. Ralph Basham with specific questions that I hope will clarify of number of issues regarding the program.[5]

At the outset, I want to state clearly that I value and strongly support CBP's efforts to screen passengers bound for the U.S. from abroad in order to identify persons "who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law."[6] Indeed, Congress has mandated that CBP conduct passenger screening, both under the Aviation and Transportation Security Act of 2001[7] and the Intelligence Reform and Terrorism Prevention Act of 2004.[8] The purpose of the screening is to ensure aviation security and, in the case of foreign citizens. to ensure that those who would do us harm or would engage in terrorist, criminal or other illegal activity are not admitted to the United States. However, any passenger screening systems utilized by CBP to achieve these legislative goals must not go beyond the letter or intent of the law by infringing upon the guaranteed rights of U.S. citizens.

I also have no objections to using automated systems for conducting name checks and performing identity-matching, as long as those systems adequately protect and control data against breaches of confidentiality and security. However, I do have some concerns about the type of data collected from passenger name records (PNR), as discussed below and with how the data collected on U.S. citizens and LPRs is analyzed, protected, shared, controlled and retained.

It has long been an established principle that when a Federal agency creates and maintains a system of records on U.S. citizens and LPRs, the Privacy Act requires that the agency must collect, use, disseminate and retain those records in the least invasive manner possible to accomplish the agency's mission.[9] In the case of CBP, that mission is border security, generally, and includes preventing terrorists from entering the United States, preventing terrorist attacks upon the United States or upon ships and airplanes traveling to the United States, and the enforcement of U.S. customs and immigration laws.

Without clear justification, however, CBP has exempted ATS-P from the Privacy Act provision that states that an agency shall only collect and maintain information about an individual that is "relevant and necessary" to accomplish a purpose required by statute or by executive order of the President to be accomplished by that agency. [10] Any government collection or record-keeping of personal data must be limited only to what is relevant and necessary to accomplish the government's authorized purpose, and that any exemptions to this rule must be narrowly applied.

---

[5] Letter from Rep. Bennie G. Thompson, Chairman-Designate of the House Homeland Security Committee, to Commissioner Basham (Dec. 28, 2006).
[6] 71 Fed. Reg. at 64544-45.
[7] 49 U.S.C 40101 et seq. *See also*, 19 C.F.R. 122.
[8] 6 U.S.C. 101 et seq.
[9] See, generally, *Doe v. Chao*, 540 U.S. 614 (2004).
[10] 5 U.S.C. 552a(e)(1).

In the SORN, the Department states that ATS was built upon the predecessor database and screening system, the Treasury Enforcement Communications System (TECS), that was covered by a previous SORN.[11] CBP has explained that TECS was originally designed as a cargo screening system for the former U.S. Customs Service, but for many years has included a comprehensive database for screening passengers as well, known as the Interagency Border Inspection System (IBIS), used by the U.S. Border Patrol. Records contained in TECS are linked to individuals and retrievable from biographical information and therefore fall within the scope of the Privacy Act. According to the "IBIS Fact Sheet," attached to the Department's ATS Privacy Impact Assessment (PIA), IBIS provides CBP access not only to CBP records but also to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications Systems (NLETS), a law enforcement database used by all fifty states.[12] Moreover, the PIA explains that, in addition to CBP, law enforcement and regulatory personnel from 20 other federal agencies use IBIS, including the FBI, Interpol, DEA, ATF, the IRS, the Coast Guard, the FAA, the Secret Service and the Animal Plant Health Inspection Service.[13] IBIS is also shared with Department of State consular officers for purposes of visa adjudication.[14] From this description, it is fair to conclude that the TECS/IBIS database is a comprehensive tool used not only for screening people and cargo at the border, but also for general law enforcement.

ATS-P apparently differs from TECS in that it automatically screens passengers based on information already contained in the TECS/IBIS database, plus the PNRs collected by airlines in the normal course of making a reservation and APIS, currently submitted within 15 minutes of takeoff.[15] I understand that ATS automatically performs two critical screening functions: 1) it checks the identity of a passenger against government watch lists, including terrorist watch lists, and 2) it performs a risk assessment of every passenger to determine if he or she "may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law." If ATS finds a possible watch list match or determines from its risk assessment that the passenger may pose a possible risk to the flight or for other terrorist or criminal activity, the record is flagged for a personal review by a CBP officer at the National Targeting Center (NTC). The reviewing CBP officer then makes a determination as to whether the passenger should receive additional scrutiny, either before he or she boards a vessel bound for the U.S. or at the U.S. port of entry upon arrival. According to CBP, the additional scrutiny may include a more rigorous screening, such as more thorough questioning or a search of the passenger's person or possessions or increased examination of his or her travel documents. The result of this additional screening may include, depending on the circumstances, refusal to board, diverting or returning an airplane already in flight, refusal to admit the passenger (if a foreign citizen) into the United States or admission and arrest of the passenger. In the case of a passenger who may be of interest to law enforcement but determined not to be a

[11] 71 Fed. Reg. at 64544.
[12] Privacy Impact Assessment, p. 29. Appendix C IBIS Fact Sheet.
[13] Id.
[14] Id.
[15] 71 Fed. Reg. 64544; Privacy Impact Assessment at p. 4.

risk to the flight itself, CBP may take other appropriate action as a "routine use" of that information, to include sharing its ATS results and underlying information with any other Federal, State or local law enforcement, regulatory, or intelligence agency. The "routine uses" listed in the SORN indicate that CBP may either push the information to another agency on its own initiative, or it may respond to any request from another agency.[16]

The SORN is overly vague in its description of which authority allows CBP to conduct this risk assessment screening. The SORN sets forth CBP's authority over border security only in the most general way. It does not adequately distinguish between CBP's legal authority and processes to use ATS to screen cargo from its legal authority and processes to screen passengers. Further, it does not distinguish between its different treatment options for foreign citizens flagged as high risk and high risk U.S. citizens, whom CBP has no authority to exclude from the United States.

The SORN also does not describe CBP's legal authority to share an ATS-P risk assessment result performed on a U.S. citizen with any Federal, State, and local law enforcement, regulatory or intelligence agency as a routine use, even in cases where CBP has determined that the citizen or LPR poses *no risk* to a flight or ship and has admitted him or her into the United States. Such a practice of routinely sharing any and all information CBP has collected on U.S. citizens and LPRs for border screening and aviation safety purposes appears to go far beyond CBP's border security mission, especially in view of CBP's decision to retain this information for up to 40 years.[17] If there are other legal authorities that permit this routine sharing of personal data of U.S. citizens and LPRs, I believe all these authorities must be specified in the SORN so citizens and LPRs, Congress and courts can better assess whether CBP or its other agency partners have exceeded that authority.

Even if such broad authority beyond border security does exist, the apparent lack of any controls or protections on the sharing of ATS-P personal data, at least as the routine uses are described in the SORN, is troubling. During the aforementioned briefings, CBP officials specifically stated that ATS-P data is only shared with other agencies at the request of the agency and only on an individual passenger or specific route basis. It was further stated that the data is not accessed on an aggregate or large-scale basis by other agencies. Notwithstanding these assurances, at a minimum, any further dissemination of this extensive personal data, either on CBP's initiative or upon request, must be documented regarding who is the requestor, what is the legal justification for receiving the data, for what purpose will the data be used, and how it will be protected from further disclosure. No such safeguards appear in the SORN. Without an established, authorized and transparent legal process to share personal data of persons protected under the Privacy Act, all the ATS data and indeed the entire TECS/IBIS database could be used as a warrantless well of evidence from which any law enforcement, regulatory or intelligence agency could dip at will -- without any probable cause, reasonable suspicion, or judicial oversight. The PIA says that Memoranda of Understanding (MOU) and other agreements are in place to govern further dissemination

[16] 71 Fed. Reg. at 64545.
[17] Id. at 64546.

outside of DHS, but, at least with respect to law enforcement, intelligence and regulatory agencies, no details of these agreements are provided.[18] Without adequate safeguards, these routine uses as described in the SORN may constitute violations of the U.S. Constitution's Fourth Amendment guarantee against unreasonable searches and seizures.

CBP has maintained, however, that U.S. citizens and LPRs should have no constitutionally protected expectations of privacy in PNR and APIS data since they freely give PNR information over to airlines when they make reservations, and APIS biographical data from passports already exist in the U.S. Government's records, such as passport records. I strongly disagree. Looking at all the many data points contained in PNR, as set out in the SORN, it is obvious that much of the collected data is exactly the kind of information that passengers desire to keep private, for example, credit card information, frequent flyer numbers, email addresses, billing and telephone numbers.[19] That this information is given to reservation agents for the sole purpose of buying a ticket in a secure business transaction does not abolish this expectation. Nor does the fact that airlines must, by law, give PNR and APIS data to CBP for the purpose of security screening change the fact that the passenger should be able to control who sees this data beyond those necessary to permit the completion of his or her travel.

In submitting a reservation request, the passenger is not relinquishing all control of their private data nor signaling that he or she wants to make this data public knowledge for all purposes. Americans and LPRs have an expectation that this information is being utilized for a discrete purpose. An expectation of privacy exists in the PNR and APIS data, and CBP is obligated to safeguard it against unwarranted disclosures. Indeed, CBP seems to acknowledge this in the SORN's description of internal safeguards it has imposed for its own personnel. There is no indication, however, that any of these safeguards apply to non-DHS law enforcement or regulatory agencies who may be tempted to troll through an individual's personal data for evidence rather than to request a proper subpoena for the information. If CBP does employs safeguards on outside disclosures as a routine use, those procedures need to be spelled out in the SORN so the public can be assured their privacy rights are not being violated.

Moreover, the breadth and detail of the PNR data raises another concern, namely, that particular data points collected and analyzed may lead to discrimination based on, for example, religion or disability, in violation of the civil rights of U.S. citizen and LPR passengers. For example, the PNR data described in the SORN would contain a request for a special meal to comply with religious dietary restrictions or a special accommodation for a disability. Both CBP officials and the DHS Chief Privacy Officer have ensured my staff that any data related to religion or disability is blocked, and thus not included in the ATS risk assessment, and the PIA supports this claim. There is nothing in the SORN, however, to indicate any restrictions on the collection of PNR data. Given the amount of detailed information that makes up PNRs, I strongly urge CBP in the interest of transparency, CBP should inform Americans which categories of data that are collected are blocked or excluded from the automated risk assessment.

---

[18] Privacy Impact Assessment, pp. 15-16.
[19] Id. at 64544.

The automated risk assessment process itself also suffers from lack of transparency. Beyond checking identities against watch lists, which would obviously flag a high risk passenger, the process and data points for flagging passengers for greater CBP scrutiny based on a computerized "risk assessment" that remains invisible to the public. As such, it has stirred understandable anxiety among citizens who have no way of assessing the objectivity or reliability of the process, which has been described as everything from data-mining to risk-scoring in the press. Oral briefings by DHS officials, have clarified that ATS-P is neither a scoring nor a data-mining process; they have described the assessment as a "flag/no flag" result based on a "links analysis," i.e., looking at links between data in the TECS, PNR and APIS data and known or suspected terrorist activity. They have explained that the relevant factors are determined by counterterrorism experts and as such, are constantly changing as facts on the ground change and more information becomes known. I was reassured that there is no indiscriminate "data-dumping" or "data-mining," but that the risk analysis evaluates each traveler for specific factors or combinations of factors that have been determined by experts to signal a need for a second look by CBP. While a good cause can be made for the non-disclosure of the relevant factors themselves, else they could be defeated, a more transparent description of the process itself would reassure Americans that their personal data is being evaluated narrowly and thoughtfully and not indiscriminately.

Another problem with the SORN is the lack of an adequate justification for retaining information collected in ATS for up to 40 years.[20] To date, no Department official has been able to provide a satisfactory explanation regarding CBP's conclusion that 40 years of data may be required "to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities."[21] Remembering that this data is collected for border security screening purposes, and not to serve as a general domestic law enforcement evidence repository, it seems patently excessive to assert that the data on every single citizen and LPR, no matter how many times they have entered and exited the country lawfully and not been "flagged," remains relevant because some link might exist between 40-year-old data and new travel.

With respect to the right to access information, the SORN seems to say that individuals will not be able to access ATS-P records on themselves to inspect them for accuracy and request modifications if inaccurate information exists.[22] This essentially exempts ATS-P from every Privacy Act provision that grants an individual the opportunity to access and correct records containing information about his or herself, again without clearly stating the justification. The PIA explains that since ATS-P collects no new information, but only uses data from other sources, individuals should seek access and redress from the various agencies that provide source data upon which ATS-P operates, such as the PNR, TECS or APIS, for example.[23] The ATS-P SORN should incorporate this explanation because, as written, a citizen is left believing there is no way

[20] 71 Fed. Reg. at 64546.
[21] Id.
[22] 71 Fed. Reg. at 64546.
[23] Privacy Impact Assessment, Sec. 7.0, pp. 16-20.

to access and seek redress for erroneous information, and the instruction to send Privacy Act inquiries to the Customer Satisfaction Unit only adds to this confusion.

Finally, the SORN does not explain how ATS-P operates with respect to passengers exiting the United States, although it repeatedly describes ATS as a system to screen inbound and outbound persons and cargo.[24] The exit portion of ATS-P should be elucidated in any revision to the SORN.

Thank you for the opportunity to file these comments. If you have any questions about these comments, please contact Jessica Herrera-Flanigan, Democratic Staff Director and General Counsel of the Committee on Homeland Security at (202) 226-2616.

Bennie G. Thompson
Chairman-Designate
Committee on Homeland Security

[24] 711 Fed. Reg. 64543-44.

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

December 4, 2006

The Honorable Michael Chertoff
Secretary
The Department of Homeland Security
Mail Stop MS 0150
Office of Legislative Affairs
Attn: Secretary
Washington, D.C. 20528

Dear Mr. Secretary:

On November 2, 2006, the Department published a Privacy Act notice in the Federal Register[1] regarding the types and uses of data collected, analyzed and retained in an automated database under the Automated Targeting System, called ATS. The notice explains that ATS conducts risk-based screening on all the information obtained from U.S. Customs and Border Protection's (CBP) cargo, travelers and border enforcement systems for the purpose of "identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law."[2]

According to the notice, data collected under ATS includes detailed personal Passenger Name Record (PNR) information provided by commercial carriers. The notice further explains that any of the data collected for screening can be shared with other civil and criminal law enforcement agencies as "routine uses,"[3] among other uses. And the data will be stored for up to 40 years.

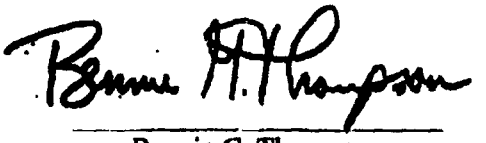
Among our many responsibilities, the Committee on Homeland Security has responsibility for oversight of the actions of the Department that may impact upon the privacy or civil rights of American citizens. After Committee staff members toured the National Targeting Center and received a briefing on ATS on December 1, serious concerns have arisen that, with respect to U.S. citizens and possibly lawful permanent aliens, some elements of ATS as practiced may constitute violations of privacy or civil rights. Reports in the media have also raised this possibility. Therefore, I believe that more time is needed for the public to comment on the implications of using ATS as set forth in the notice and request that you extend the comment period until January 8, 2007.

---

[1] 71 FR 64543-6.
[2] Id at 64545.
[3] Id.

Certainly, the Department needs to identify persons traveling to the United States who may be terrorists, criminals, or may engage in other activity in violation of U.S. law; however, the systems must be designed in a manner as not to violate the rights of U.S. citizen travelers, especially, and must be balanced against overly-expansive collection, analysis and retention of personal data. Thank you, in advance, for your timely consideration of this request. Please contact Jessica Herrera-Flanigan at 202.226.2616 on my staff, should you have questions or concerns about this request.

Sincerely,



Bennie G. Thompson
Ranking Member
Committee on Homeland Security

(b6)

From: Agen, Jarrod

Sent: Friday, December 08, 2006 2:00 PM

To: (b6); Knocke, William R; Kraninger, Kathleen; Sweet, Chad; (b6) Kent, Don; Snyder, Jack; Sales, Nathan; Baker, Stewart; Rosenzweig, Paul; Levy, Andrew; Coldebella, Gus; Perry, Phil; (b6) Ahern, Jayson P; (b6) (b6) Isles, Adam; Teufel, Hugo; (b6)

Cc: (b6) Klundt, Kelly R; Frawley, Anne Marie

Subject: JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Attachments: Just the Facts ATS.doc

Thanks for all the input. This is the final version. We will be retailing this out to reporters, feel free to push out as needed.

Press Office
U.S. Department of Homeland Security

Just The Facts

Dec 8. 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

AN ASSOCIATED PRESS STORY CLAIMS THAT THE AUTOMATED TAGERTING SYSTEM (ATS) MAY VIOLATE U.S. LAW: "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT IT IS CLEAR THAT CONGRESS DID NOT INTEND TO LIMIT THE ATS PROGRAM:

- The Aviation and Transportation Security Act of 2001 mandates that each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to Customs an electronic transmission of a passenger manifest and carriers shall make passenger name record information available to the Customs Service.

THE STORY CLAIMS A PROVISION BY CONGRESS PROHIBITS COMPUTERIZED RISK ASSESSMENTS: "But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT WHEN READ IN CONTEXT, IT IS CLEAR THAT THE PROVISION WHICH SOME HAVE SUGGESTED WAS ADDED TO REGULATE ATS (SECTION 514 OF THE DHS APPROPRIATIONS BILL), HAS NOTHING TO DO WITH ATS, NOR WAS IT INTENDED AS A CATCH-ALL PROVISION:

- The various sections of the law cannot be read in isolation. Section 514 is concerned only with aviation security generally and the Secure Flight program administered by TSA in

particular. Congress did not intend section 514 to pertain to ATS, a program that has been funded by Congress since the late 1990's and has an entirely different mission from Secure Flight. Secure Flight is intended to screen domestic passengers attempting to board airplanes, while ATS relates to individuals seeking admission to the U.S. at ports of entry.

- ATS has been in existence since the late 1990's. Congress is presumed to be aware of programs in existence when it passes legislation. The fact that Congress makes no mention of ATS undermines the suggestion that it intended to regulate it in any way. Because ATS predates the Secure Flight program, it can be neither a "follow-on" nor "successor" program to Secure Flight, as required by section 514(a).

- Furthermore, the provision prohibits the use of DHS funds "for data or a database that is obtained from or remains under the control of a non-Federal entity," except Passenger Name Record Data obtained from air carriers. This provision only makes sense if it is limited to testing activities for Secure Flight. Otherwise, by this language, Congress would have made illegal any use of non-Federal database material by the federal government, thereby shutting down numerous legitimate programs having nothing to do with aviation security.

THE STORY ALSO CLAIMS THAT THERE HAS BEEN LITTLE NOTICE OF ATS: "ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules. *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT DEPARTMENT OFFICALS HAVE TESTIFIED BEFORE CONGRESS SEVERAL TIMES AND HAVE PROVIDED NUMEROUS STAFF BRIEFINGS AND TOURS OF THE ATS AND THE OPERATIONS AT THE NATIONAL TARGETING CENTER.

- Excerpts from the nearly 20 written testimony about ATS to Congress since May 2003 include:

➢ **DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006):** "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags." and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

➢ **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006):** "The Automated Targeting System. which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases. overseas."

➢ **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006):** "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify

(DC hid)

those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

- **Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004):** "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

- **CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004):** The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

(oa la:)

Press Office
U.S. Department of Homeland Security

Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

AN ASSOCIATED PRESS STORY CLAIMS THAT THE AUTOMATED TAGERTING SYSTEM (ATS) MAY VIOLATE U.S. LAW: "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT IT IS CLEAR THAT CONGRESS DID NOT INTEND TO LIMIT THE ATS PROGRAM:

- The Aviation and Transportation Security Act of 2001 mandates that each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to Customs an electronic transmission of a passenger manifest and carriers shall make passenger name record information available to the Customs Service.

THE STORY CLAIMS A PROVISION BY CONGRESS PROHIBITS COMPUTERIZED RISK ASSESSMENTS: "But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists." *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT WHEN READ IN CONTEXT, IT IS CLEAR THAT THE PROVISION WHICH SOME HAVE SUGGESTED WAS ADDED TO REGULATE ATS (SECTION 514 OF THE DHS APPROPRIATIONS BILL), HAS NOTHING TO DO WITH ATS, NOR WAS IT INTENDED AS A CATCH-ALL PROVISION:

- The various sections of the law cannot be read in isolation. Section 514 is concerned only with aviation security generally and the Secure Flight program administered by TSA in particular. Congress did not intend section 514 to pertain to ATS, a program that has been funded by Congress since the late 1990's and has an entirely different mission from Secure Flight. Secure Flight is intended to screen domestic passengers attempting to board airplanes, while ATS relates to individuals seeking admission to the U.S. at ports of entry.

- ATS has been in existence since the late 1990's. Congress is presumed to be aware of programs in existence when it passes legislation. The fact that

Congress makes no mention of ATS undermines the suggestion that it intended to regulate it in any way. Because ATS predates the Secure Flight program, it can be neither a "follow-on" nor "successor" program to Secure Flight, as required by section 514(a).

- Furthermore, the provision prohibits the use of DHS funds "for data or a database that is obtained from or remains under the control of a non-Federal entity," except Passenger Name Record Data obtained from air carriers. This provision only makes sense if it is limited to testing activities for Secure Flight. Otherwise, by this language, Congress would have made illegal any use of non-Federal database material by the federal government, thereby shutting down numerous legitimate programs having nothing to do with aviation security.

THE STORY ALSO CLAIMS THAT THERE HAS BEEN LITTLE NOTICE OF ATS: "ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules. *("Traveler Risk System May Violate Ban", Associated Press 12/7/06)*

BUT DEPARTMENT OFFICALS HAVE TESTIFIED BEFORE CONGRESS SEVERAL TIMES AND HAVE PROVIDED NUMEROUS STAFF BRIEFINGS AND TOURS OF THE ATS AND THE OPERATIONS AT THE NATIONAL TARGETING CENTER.

- Excerpts from the nearly 20 written testimony about ATS to Congress since May 2003 include:

➢ **DHS Deputy Secretary Michael P. Jackson, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee (April 5, 2006):** "ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry."

➢ **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Hearing before Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations (March 28, 2006):** "The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas."

- **CBP Assistant Commissioner Jayson Ahern, Written Testimony, Senate Committee on Judiciary, Subcommittee on Terrorism, Technology, and Homeland Security (September 7, 2006)**: "Next, we'd like to highlight some of the steps DHS takes to screen airline passengers and prevent the dangerous ones from boarding U.S.-bound aircraft. Throughout the travel and arrival processes, a host of Customs and Border Protection resources are marshaled to obtain and analyze information about every traveler, identify those who are likely to present a higher risk, and interdict and further screen those who are deemed high risk. At the core of this effort is the National Targeting Center (NTC). NTC receives inbound and outbound passenger information and runs it against sophisticated risk assessment rules and algorithms in the Automated Targeting System (ATS). ATS's methodologies are based on strategic intelligence about the terrorist threat, and ATS compares passenger information against data from numerous national intelligence and law enforcement databases, including the combined Federal law enforcement database known as the Treasury Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS) and the National Crime Information Center (NCIC) database. The analysis NTC conducts on inbound passengers is largely based on two sources of information – Advance Passenger Information (API) and Passenger Name Records (PNR). Both types of information are used to prevent and combat terrorism and terrorist acts, as well as to catch persons suspected of other serious crimes. CBP also uses this information to facilitate bona fide travelers so it can focus its resources on areas of highest risk."

- **Former CBP Commissioner Robert Bonner, Written Testimony, Hearing before House Appropriations Committee, Subcommittee on Homeland Security (March 25, 2004):** "The Automated Targeting System (ATS), which is used by NTC and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to pick up anomalies and "red flags" and determine what cargo is "high risk," and therefore will be scrutinized at the port of entry or, in some cases, overseas.

- **CBP Executive Director, Traveler Security and Facilitation, Robert Jacksta, Written Testimony, Hearing before House Committee on Government Reform, Subcommittee on National Security, Emerging Threats and International Relations (July 13, 2004):** The Automated Targeting System-Passenger (ATS-P) is CBP's premier targeting tool in the passenger environment, and is available to CBP personnel at U.S. ports of entry nationwide. This system utilizes information from the National crime Information center (NCIC), the Treasury Enforcement Communications System (TECS), the Consular Lookout and Support System (CLASS) and other law enforcement databases to provide automated risk assessments on arriving international passengers.

(b6)

From: Teufel, Hugo (b2)

Sent: Friday, December 08, 2006 1:31 PM

To: Rosenzweig, Paul; Levy, Andrew; Coldebella, Gus; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b6); Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; (b6); Ahern, Jayson P; (b6)

Cc: (b6) Klundt, Kelly R

Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Importance: High

The transcript of the DPIAC June 2005 morning meeting has a quote from Paul talking about automated targeting, as had been briefed to the committee the day earlier. It was in the morning session, and can be found here:

http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_trans_am.pdf

Paul asks the question and Robert Jacksta responds. See pages 26 and 27. Paul first:

> I guess I'm going to take the Chairman's privilege of the first question, and screen Mr. Jacksta. We learned yesterday about the automated tracking, targeting center, and in particular, we learned that it was operating under a legacy, privacy impact statement since it initiated before the Privacy Act came into existence even. It seemed to me, from the way it was described, it changed its function quite a bit, post 9/11, as it should, to reflect the terrorists, the changing terrorist's flight.
>
> So I was wondering if you were planning on going through the process of developing another privacy impact assessment, statement for it, if not, why not, and if so, when?

The response from Jacksta is:

> MR. JACKSTA: I think the best way to answer that question is, obviously, it's something that we need to continue to look at, and if there's a need to make sure that we're in compliance with the Privacy Act and the Privacy Impact Statements, then we'll do that and work very closely with the Privacy Office to make sure that we accomplish that.
>
> I think what is important to note was that the systems that you saw running yesterday were systems that were in place well before 2001. They weren't defined as they are today and obviously we have better rules, we have a better system, but before 2001, we were receiving a APIS information, we were using passenger name record information, we were using an automated targeting system that allowed us to bring all that information together. Over the years, over the last three or four years we have made improvements on that to allow us to, first of all, process additional information quicker and faster and get better results back to the officer in easier format for them to read.
>
> The legacy systems that we have brought together that are now being worked --to establish the right connectivity to the officers are legacy systems that were out there for our officers before, whether they were immigration or customs, so I'll bring that question back. I can't specifically answer if we need to

have a new privacy impact statement, but I do know that we work very closely with the Privacy Office, with our counsel to make sure that we're in compliance, that's extremely important to us.

Hugo Teufel III
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, DC 20528
(b6)

From: Rosenzweig, Paul
Sent: Friday, December 08, 2006 1:05 PM
To: Levy, Andrew; Coldebella, Gus; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b6) Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; (b6) A; Ahern, Jayson P
Cc: (b6) Teufel, Hugo
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

(b5) ... back when I was chair of the Data Privacy Advisory Committee (a public body) in June 2005, CBP took the members on a tour of the Boston targeting unit and all of this was very clear. Jacksta testified before us the next day and his testimony was also clear, though a bit more guarded.

(b5)

P

From: Levy, Andrew (b6)
Sent: Fri 12/8/2006 12:30 PM
To: Coldebella, Gus; Levy, Andrew; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b6); Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; Atkiss, Steve A; Ahern, Jayson P
Cc: (b6) Klundt, Kelly R
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

[b5]

(b6 b7C)

[b5]

Andrew J. Puglia Levy
Associate General Counsel (Legal Counsel)
U.S. Department of Homeland Security
[b2] (work)
(cell)
(fax)
(b2)

-----Original Message-----
From: Coldebella, Gus (b2)
Sent: Friday, December 08, 2006 12:29 PM
To: Levy, Andrew; Sales, Nathan; Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; (b6)
(b6); Coldebella, Gus; Perry, Phil; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; (b6); Ahern, Jayson P
Cc: (b6); Klundt, Kelly R
Subject: Re: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

[b5]

----- Original Message -----
From: Levy, Andrew (b2)
To: Sales, Nathan [b2]; Kraninger, Kathleen [b2]
AGEN, JARROD <[b2]; Knocke, William R <[b2]
(b6) (b2) Coldebella, Gus (b2); Perry,
Phil (b2) Levy, Andrew (b2) Isles, Adam
(b2) Baker, Stewart (b2) Rosenzweig, Paul
(b2) Scardaville, Michael (b2) (b6)
Ahern, Jayson P
Cc: (b6); Klundt, Kelly R
Sent: Fri Dec 08 12:15:55 2006
Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

[b5]

(b2 b6)

[b5]

Andrew J. Pugliа Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

[b2] (work)

(cell)

(fax)

(b2)

(b2-low)

-----Original Message-----
From: Sales, Nathan (b6)
Sent: Friday, December 08, 2006 12:11 PM
To: Kraninger, Kathleen; AGEN, JARROD; Knocke, William R; Bergman, Cynthia; Coldebella, Gus; Perry, Phil; Levy, Andrew; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Sales, Nathan; Scardaville, Michael; (b6) Ahern, Jayson P
Cc: (b6) Klundt, Kelly R
Subject: Re: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

(b5)

Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Kraninger, Kathleen (b2).

To: Agen, Jarrod (b2); Knocke, William R (b2) (b6) (b2) Coldebella, Gus (b2) Perry, Phil (b2) Levy, Andrew (b2) Isles, Adam (b2) Baker, Stewart (b2) Rosenzweig, Paul [b2]; Sales, Nathan (b2) Scardaville, Michael [b2] Kraninger, Kathleen (b2) (b6) Ahern, Jayson P

Cc: (b6) Klundt, Kelly R

Sent: Fri Dec 08 12:07:48 2006

Subject: RE: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Testimony on ATS goes back farther. (b5]
(

From: Agen, Jarrod (b2)

Sent: Fri 12/8/2006 12:04 PM

(b2 b5)

To: Knocke, William R; (b6) ; Coldebella, Gus; Perry, Phil; Levy, Andrew; Isles, Adam; Baker, Stewart; Rosenzweig, Paul; Sales, Nathan; Scardaville, Michael; Kraninger, Kathleen; Atkiss, Steve A; Ahern, Jayson P

Cc: (b6) ; Klundt, Kelly R

Subject: draft JUST THE FACTS: ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

Please review this JUST THE FACTS response to AP article. Let me know if there are any errors or changes to be made. We will push it out in an about an hour.

Press Office

U.S. Department of Homeland Security

Just The Facts

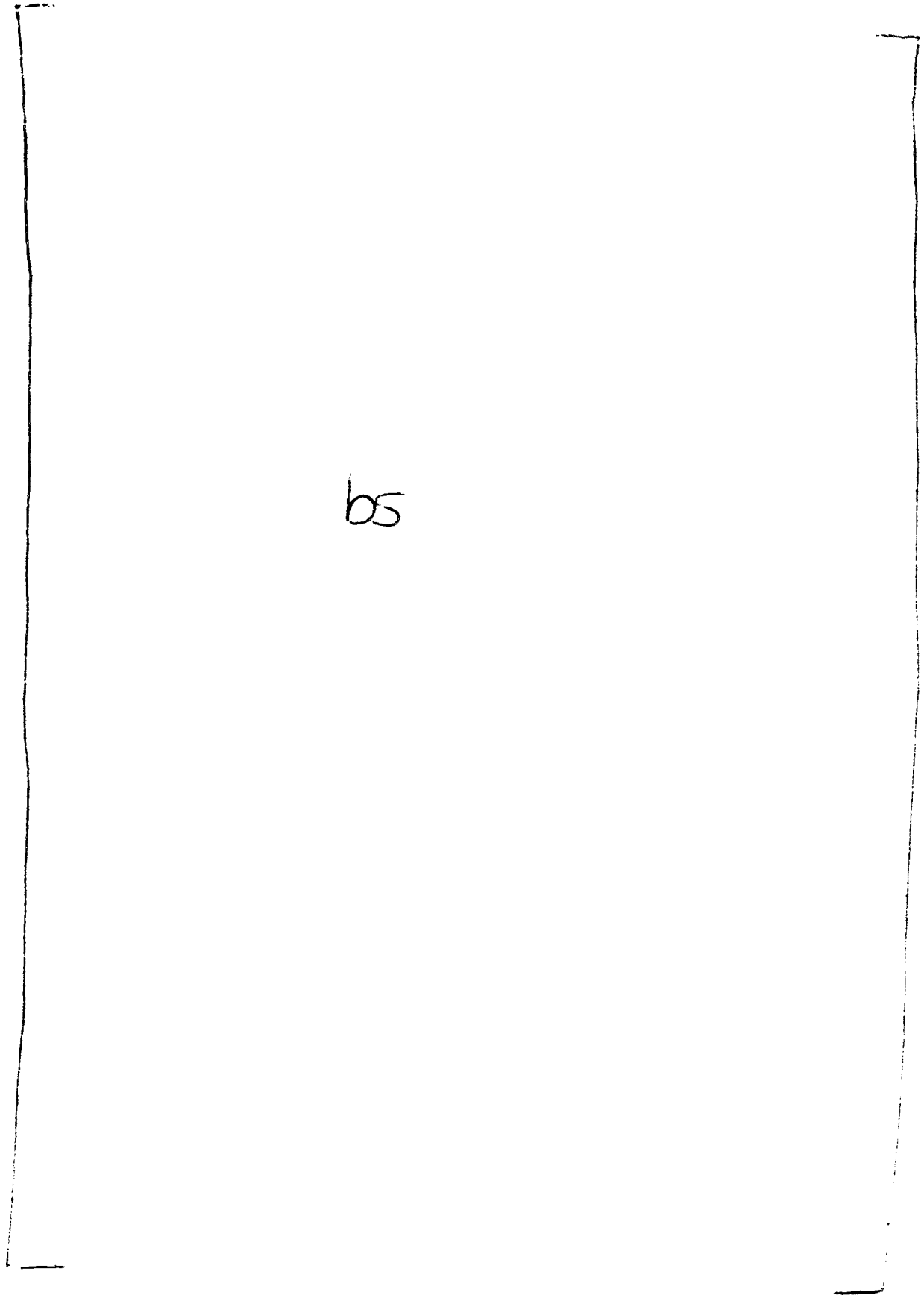
Dec 8, 2006

ASSOCIATED PRESS ON AUTOMATED TARGETING SYSTEM

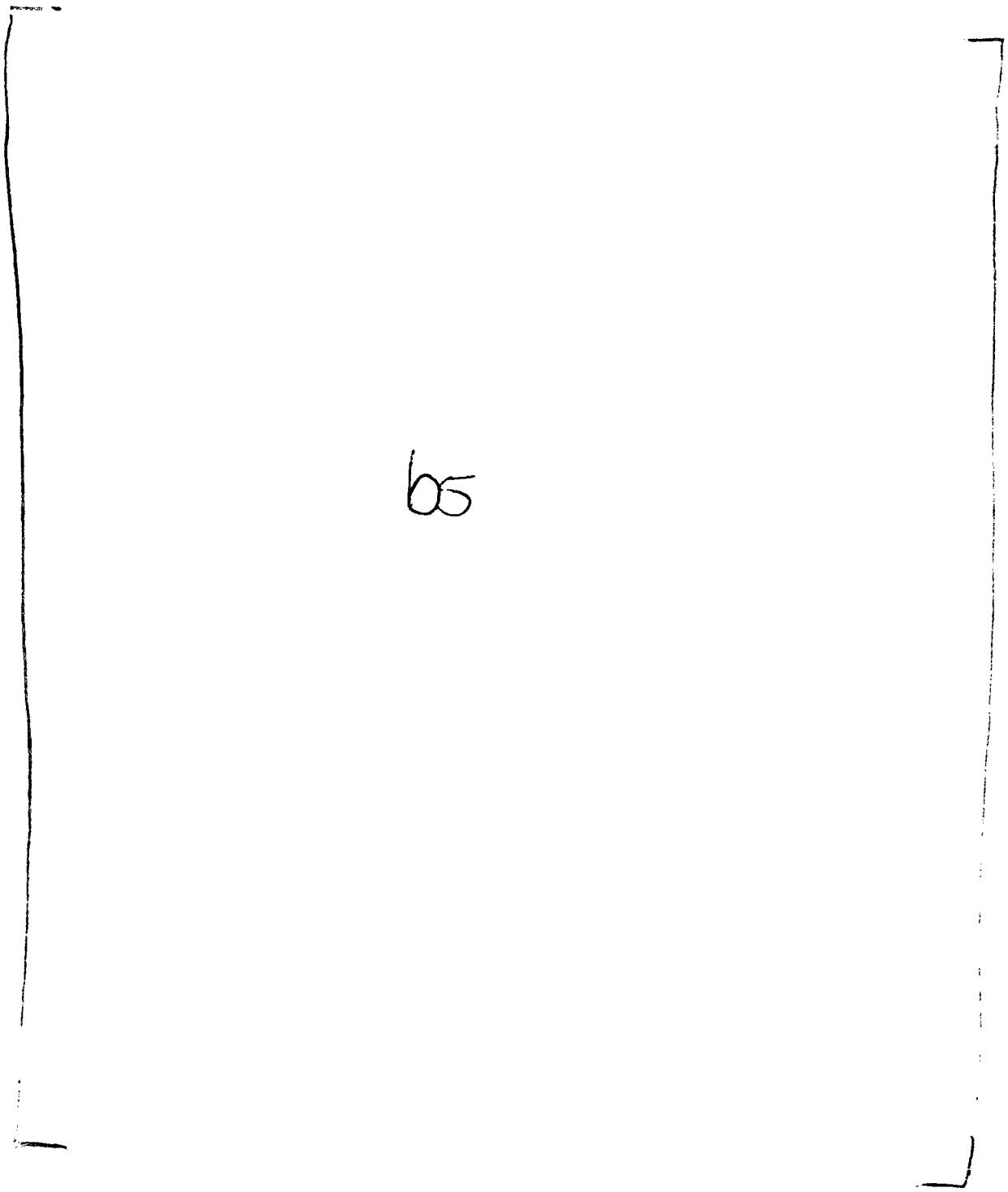
(b3 b6)

65

65



(b2(a1))



(n260)

(balow)

(b6)

From: Baker, Stewart (b2)
Sent: Wednesday, December 13, 2006 1:28 PM
To: (b6 ; Levy, Andrew; Isles, Adam; AGEN. JARROD; Baker, Stewart; White, Brian M; Rosenzweig, Paul; Sales, Nathan; Coldebella, Gus; (b6)
Cc: Knocke, William R; (b6); Kraninger, Kathleen
Subject: Re: EU press release on ATS/PNR

(b5)

Stewart Baker
Typed with my thumbs, so please make allowances for curtness and typos.

----- Original Message -----
From: (b6) (b2)
To: Levy, Andrew (b2) Isles, Adam (b2) Agen. Jarrod (b2); Baker. Stewart (b2) White, Brian M (b2) Isles, Adam (b2) Rosenzweig, Paul (b2); Sales, Nathan (b2) Coldebella, Gus (b2) (b6) (b2) (b6)
Cc: Knocke. William R (b2) (b6) (b2) Kraninger, Kathleen (b2)
Sent: Wed Dec 13 13:18:09 2006
Subject: RE: EU press release on ATS/PNR

[b5]

(b6)
Senior Attorney
Office of Chief Counsel
U.S. Customs and Border Protection
Phone: (b2)
Fax: (b2)
email: (b2)

-----Original Message-----
From: Levy, Andrew (b2)
Sent: Wednesday, December 13, 2006 1:08 PM
To: Isles, Adam; Agen, Jarrod; Baker, Stewart; White, Brian M; Isles,

(b6)

Adam; Rosenzweig, Paul; Sales, Nathan; Coldebella, Gus; (b6)
(b6)
Cc: Knocke, William R; (b6) Kraninger, Kathleen
Subject: RE: EU press release on ATS/PNR

[redacted]

b5

Andrew J. Puglia Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

[redacted] (work)

(cell)

(fax)

( )

From: Isles, Adam
Sent: Wednesday, December 13, 2006 11:54 AM
To: Agen, Jarrod; Baker, Stewart; White, Brian M; Isles, Adam; Rosenzweig, Paul; Sales, Nathan; Coldebella, Gus; Levy, Andrew; ( )
( )
Cc: Knocke, William R; ( ) ; Kraninger, Kathleen

( )

Subject: RE: EU press release on ATS/PNR

Looping in OGC too ...

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

(b2) tel

From: Agen, Jarrod [mailto: (b2)
Sent: Wednesday, December 13, 2006 11:52 AM
To: Baker, Stewart; White, Brian M; Isles, Adam; Rosenzweig, Paul; Sales, Nathan
Cc: Knocke, William R; (b6); Kraninger, Kathleen
Subject: EU press release on ATS/PNR
Importance: High

EU pushed out this release today - getting several press calls here.

Given this is out of Frattini's office - do you have guidance on how you want me to push back?

Are we confident that ATS system is covered in Undertakings?

From: Strohm, Chris [mailto:CStrohm@nationaljournal.com]
Sent: Wednesday, December 13, 2006 11:42 AM
To: AGEN, JARROD; Knocke, William R
Subject: Seeking immediate comment for story
Importance: High

Russ, Jarrod: I'm sorry for the short notice but I literally just got this. The EU today issued a statement on how PNR data is being used in the Automated Targeting System.

It says: "The information published by the DHS reveals significant differences between the way in which PNR data are handled within the Automated Targeting System on the one hand and the stricter regime for European PNR data according to the Undertakings given by the DHS."

The EU is sending DHS a letter asking for clarification and hints that this all could negatively affect renewal of the PNR agreement.

(b2 b6)

I'm doing a story on this for today. My deadline is 1:30pm. Again, sorry for the late notice but this literally just broke. Please email me or call me at 202-413-2212 with comment. The EU's full statement follows below. Chris

*****

This is a press release from the European Commission
Vice President Franco Frattini
European Commissioner responsible for Justice, Freedom and Security

"Data protection and transfer of PNR data"

European Parliament

Strasbourg, 13 December 2006

On 19th October the European Union and the United States concluded an agreement for the processing and transfer of passenger name record data by air carriers to the United States Department of Homeland Security. The US Government confirmed a set of Undertakings which guarantee the protection and security of PNR data.

Against this background concern has been expressed in recent days following information published last month by the Department of Homeland Security on the "Automated Targeting System". This is a security screening system making a risk assessment of international travellers relying, among other things, on PNR data. The information published by the DHS reveals significant differences between the way in which PNR data are handled within the Automated Targeting System on the one hand and the stricter regime for European PNR data according to the Undertakings given by the DHS.

The Council Presidency and Commission have sent today a letter to the US Government to request formal confirmation that the way EU PNR data are handled in the ATS is the one described in the Undertakings.

The current EU-US Agreement on PNR data will expire in July of next year. The Commission will, at the beginning of 2007, recommend to Council to mandate the Presidency, assisted by the Commission, to negotiate a new PNR agreement with the United States. I am sure that any new agreement will provide for a high level of data protection for all PNR data transferred under the agreement while protecting the security of our citizens.

I will keep the EP informed about the mandate and the progress of negotiations. COM expects to receive a mandate from Council before March next year.

I have always taken the position that travellers must be informed when their PNR data may be transferred to competent authorities of third countries. The DHS Undertakings expressly acknowledge this. We need an international agreement with the support of the public on both sides of the Atlantic and of the democratic representatives of the peoples.

I have often said that there is an important balance to be struck between measures to ensure security on the one hand and the protection of non-negotiable fundamental rights on the other. The Commission, assisting the Presidency in the negotiation of future PNR agreements with third countries, will ensure that security issues are properly addressed through the transfer and appropriate use of PNR data, while

(62/64)

protecting personal data guaranteed by Article 8 of the Charter of Fundamental Rights.

Finally, a high level Contact Group was set up at the EU-US JLS Ministerial troika on 6 November 2006 to discuss information sharing and protection of personal data for law enforcement purposes. There is a clear need on both sides of the Atlantic to work more closely together on these issues.

I would personally be in favour of close contacts between the above High Level Group and both the European Parliament and the US Congress.

We need a broader perspective and a long-term vision to tackle, together with the US, the terrorist threat without putting at risk the fundamental rights of individuals.

I am also firmly committed to continue encouraging the Council to make progress on the Framework Decision on data protection in the Third Pillar. I hope the incoming German Presidency will be able to make substantial progress on that.

We do have a common problem and threat - terrorism - which will continue to exist in the coming months and years. Only a very solid strategy, and a balanced cooperation with our main international transatlantic partner, will allow reducing, if not eliminating, this modern form of 'totalitarianism' against democracy.

(b6)

From: Knocke, William R (b6)
Sent: Friday, December 08, 2006 8:41 PM
To: (b6) Sweet, Chad; Perry, Phil; Coldebella, Gus; Baker, Stewart; Rosenzweig, Paul; Isles, Adam; Levy, Andrew
Cc: Agen, Jarrod
Subject: Time MAG: Airline "Risk Assessment": Defending the Right to Snoop

Airline "Risk Assessment": Defending the Right to Snoop

Should federal agents know where you sit on an airplane and what kind of meal you order? Homeland Security Chief Michael Chertoff says yes

By SALLY B. DONNELLY

The Department of Homeland Security's Automated Targeting System has become a key part of the nation's air security system. Rather than just checking a list of passenger names for those who might be suspected of terrorist activities, it applies a"risk assessment"to every airline passenger entering the U.S. by using more than two dozen criteria, including how the airline ticket was bought, contact phone numbers provided, and frequent flier information. ATS even wants to know your seat preference. The ATS data is fed to the National Targeting Center, a multi-agency center that crunches the data against criminal databases and watch lists. If your data raises too many concerns, or some questions can't be answered, you'll receive a"red flag"and be pulled aside for questioning by a Customs and Border Patrol agent.

But ATS, which was recently upgraded after a new agreement on international standards with European countries, has come under increased criticism for knowing too much, being too secret, and not allowing passengers any recourse to challenge their risk assessments. This week, the DHS extended the deadline for public comment on the ATS system: most of the complaints have attacked the system on privacy grounds. The Identity Project, a privacy-rights group, has alleged that the ATS data collection is illegal. It claims that "Congress has expressly forbidden the DHS from spending a penny on any system like this to assign risk scores to airline passengers, and that the Privacy Act forbids any Federal agency from collecting information about how we exercise rights protected by the First Amendment - like our right to travel - except as expressly directed by Congress."

The outcry has grown loud enough to bring out DHS officials for an aggressive counterattack. DHS Secretary Michael Chertoff, who weighed in with an op-ed article in the Washington Post this week, told TIME in an interview that the ATS program is an "essential" way to look for the connections that terrorists have used in the past before they struck. "The ATS system", Chertoff says, "allows us to see connections like terrorists have known to have in the past and analyze them before something happens." Chertoff asserts that if this kind of data mining had been in place before Sept. 11, federal authorities might have well known about the connections among the hijackers. Alleged 20th hijacker, Zacarias Moussaoui, for example, used the same contact telephone number as some of the Sept. 11 hijackers. "The bottom line, from all I have seen, is that if we don't have this ability, we might as well blindfold our agents."

According to DHS, ATS was the primary means used to bar 565,417 people from entering the U.S last year; 493 of them were found to be inadmissible under "suspicion of terrorist or security grounds." And thousands were turned back because DHS couldn't quite be sure who they were. In fiscal year 2005, more than 84,000 individuals were apprehended at the ports of entry trying to cross the border with fraudulent claims of citizenship or documents. Unlike other parts of the nation's air security system, the ATS program is run not by the Transportation Security Administration — the organization that provides the 40,000 white-shirted screeners at the country's 400 largest airports but has been plagued by missteps and failures — but by the department of Customs and Border Protection.

(b2 low)

Chertoff defends even aspects of the ATS data collection that might be deemed trivial and a needless invasion of privacy. In certain cases, for example, the U.S. can obtain the meal preferences of a passenger. Chertoff points out that such cases require special high-level approval from both the U.S. and international law enforcement authorities. The point, says Chertoff, is to use all the tools we have to act before the terrorist do. "If we sit back and just rely on a list of names, we will likely miss something. And we do not want to be in that position ever again."

Russ Knocke
Press Secretary
Department of Homeland Security
Office: [b2]
Cell:
Fax:

(b6)

From: Baker, Stewart
Sent: Friday, December 15, 2006 5:27 PM
To: Isles, Adam; Coldebella, Gus; (b6)
Cc: Levy, Andrew; Barth, Richard; Sales, Nathan
Subject: RE: ATS-P -- some possible shifting tactics by the ACLU et al

Very helpful. We're getting the same signals from Hill staff. (b5)

At the same time, if there's a consensus that we aren't worried about the privacy of foreigners, perhaps Congress will authorize us to compel production of travel records from, say, Waziristan to Indonesia.

From: Isles, Adam
Sent: Friday, December 15, 2006 2:52 PM
To: Coldebella, Gus; Baker, Stewart; (b6)
Cc: Levy, Andrew; Barth, Richard; Sales, Nathan
Subject: FW: ATS-P -- some possible shifting tactics by the ACLU et al

Some further thoughts on ATS from Brian Goebel, who advised Commissioner Bonner on targeting.

I might add an additional point to Brian's note below on rationale for putting USCs through ATS: we may not be able to exclude USC entry into the country, but we can keep their contraband luggage (weapons, etc.) from coming in, and we need tools to help us make these assessments.

Adam Isles
Counselor to the Secretary
U.S. Department of Homeland Security
(b2) tel

From: (b6) (b2)
Sent: Friday, December 15, 2006 7:00 AM
To: 'Isles, Adam'
Cc: 'Josh Kussman'
Subject: ATS-P -- some possible shifting tactics by the ACLU et al

Adam,

I was invited to speak to the attorneys at Gibson Dunn yesterday. Not surprisingly, the issue of ATS-P came up. I ended up in a very spirited exchange with one of the more liberal members of the firm, and someone who may be piped into the ACLU. The interesting point in the exchange was this: he ultimately agreed that the government could perform risk assessments and store data on non-US citizens. He also seemed to recognize that the government could perform risk assessments on US citizens (although he didn't fully accept the need for this, suggesting that USCs weren't going to commit attacks in the U.S.). But he thought that the government should not be allowed to store data on USCs or use the risk assessment on USCs for any other purpose.

I raise this dialogue because I think it may help you prepare for the issues that are going to come up in the Congress and it may give some insight into where much the ATS-P debate is going to be fought – what to do about USCs. And, my debate really identified two separate issues: (1) what is the legal authority/what are the legal prohibitions on collecting and using information on USCs; and (2) what are the policy arguments that would support collecting and using this data on USCs. I think the legal arguments are pretty strong. Border search authority (the general authority) and ATSA (the specific authority) do not distinguish in CBP's ability to search

(b2 b6)

(i.e., obtain information from) USCs and non-USCs, although I have not researched the case law to confirm that view. I would encourage you to have the Department prepare a pocket brief on that point, if you haven't already done so. Second, what are the policy arguments for risk-assessing USCs and storing data on USCs (even if they are assessed as no risk)? I pointed out that there have been plenty of USCs involved in terrorism, although I couldn't remember all the names. And, I pointed out that just because a person is judged as no threat in 2006 doesn't mean he or she won't be a threat in 2015, and therefore maintaining some relatively innocuous travel history information on people is justifiable. This, ultimately, may be where the ACLU (and Members of Congress) are going to argue most strongly against ATS-P. Some people believe this is Hoover's FBI all over again.

In any event, I wanted you to have this information as you continue to plot strategy on this issue. Good luck,

(b6)

(b2 b6)

(b6)

From: Spero, Deborah J
Sent: Thursday, December 07, 2006 8:27 PM
To: Isles, Adam; (b6) Isles, Adam
Cc: Levy, Andrew; Coldebella, Gus; (b6) Robles, Alfonso; (b6 & b2)
Subject: RE: ACLU 514(e) Points

As per my recent e-mail, the FY 07 report appropriated $27M. I am going to ask (b6) to provide the previous approps tomorrow.

-----Original Message-----
From: Isles, Adam [mailto: (b2]
Sent: Thursday, December 07, 2006 8:15 PM
To: (b6) SPERO, DEBORAH J; Isles, Adam
Cc: Levy, Andrew; Coldebella, Gus
Subject: Re: ACLU 514(e) Points

Can we get those reports (tomorrow am)?

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: (b6) (b2)
To: Spero, Deborah J; Isles, Adam (b6)
Sent: Thu Dec 07 19:33:22 2006
Subject: FW: ACLU 514(e) Points

Sorry, I did not read you in earlier when I sent to Mr. Levy.

From: (b6)
Sent: Thursday, December 07, 2006 7:12 PM
To: Levy, Andrew; AHERN, JAYSON P; (b6 & b2)
(b6)
Subject: FW: ACLU 514(e) Points

[b5]

From:
[mailto [b6 & b2
Sent: Thursday, December 07, 2006 6:34 PM
To: (b6)
Subject: Fw: ACLU 514(e) Points

(b2 low)

Sent from my BlackBerry Handheld.

----- Original Message -----
From: "Coldebella, Gus" (b2)
Sent: 12/07/2006 06:29 PM
To: "Isles, Adam" (b2) "Levy, Andrew" (b2) "Rosenzweig, Paul" (b2) "Agen, Jarrod" (b2) 'Coldebella, Gus" [b2] "Kraninger, Kathleen" ; "Spero, Deborah J" (b2) "Ahern, Jayson P" (b2)
Cc: "Knocke, William R" (b2) (b6) (b2)
Subject: RE: ACLU 514(e) Points

We're putting together more full talkers now-will include.

Gus P. Coldebella

Deputy General Counsel

Office of the General CounselYes, these are correct. The only addition I can recommend (
[b5]

U.S. Department of Homeland Security

(b2) (office)

(b6) (mobile)

From: Isles, Adam [mailto: (b2)]
Sent: Thursday, December 07, 2006 6:30 PM
To: Levy, Andrew; Rosenzweig, Paul; Agen, Jarrod; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen; Spero, Deborah J; Ahern, Jayson P
Cc: Knocke, William R; (b2)
Subject: ACLU 514(e) Points

[b5]

(b2 b7)

2. Looping in CBP

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

(b2) - tel

From: Levy, Andrew [mailto: (b2)]
Sent: Thursday, December 07, 2006 5:36 PM
To: Rosenzweig, Paul; Agen, Jarrod; Levy, Andrew; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen
Cc: Knocke, William R: (b6).
Subject: RE: ATS wash post question

Thoughts?

* * *

[b5]

(b2 b5)

[b5]

Andrew J. Puglia Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

[b2] (work)

(cell)

(fax)

(b2)

(b2b2)

(b6)

From: (b6)
Sent: Thursday, December 07, 2006 8:21 PM
To: Isles, Adam; Spero, Deborah J; Isles, Adam; Ahern, Jayson P; (b6)
Cc: Levy, Andrew; Coldebella, Gus
Subject: RE: ACLU 514(e) Points

Yes, we should be able to obtain in the AM.

-----Original Message-----
From: Isles, Adam [mailto: (b2)]
Sent: Thursday, December 07, 2006 8:15 PM
To: (b6); SPERO, DEBORAH J; Isles, Adam
Cc: Levy, Andrew; Coldebella, Gus
Subject: Re: ACLU 514(e) Points

Can we get those reports (tomorrow am)?

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: (b6) (b7)
To: Spero, Deborah J; Isles, Adam (b2)
Sent: Thu Dec 07 19:33:22 2006
Subject: FW: ACLU 514(e) Points

Sorry. I did not read you in earlier when I sent to Mr. Levy.

From: (b6)
Sent: Thursday, December 07, 2006 7:12 PM
To: Levy, Andrew; AHERN, JAYSON P; (b6 ¶ b2)
(b6)
Subject: FW: ACLU 514(e) Points

Yes, these are correct. The only addition I can recommend (

[b5]

From:
[mailto:, [b6 ¶ b2]
Sent: Thursday, December 07, 2006 6:34 PM
To: (b6)
Subject: Fw: ACLU 514(e) Points

Sent from my BlackBerry Handheld.

(b2/b7)

----- Original Message -----
From: "Coldebella, Gus" (b2)
Sent: 12/07/2006 06:29 PM
To: "Isles, Adam" (b2) "Levy, Andrew" (b2) "Rosenzweig, Paul" (b2) "Agen, Jarrod" (b2) "Coldebella, Gus" (b2) "Kraninger, Kathleen" (b2) Spero, Deborah J" (b2) "Ahern, Jayson P" (b2)
Cc: "Knocke, William R" (b2) (b2) (b2)
Subject: RE: ACLU 514(e) Points

We're putting together more full talkers now-will include.

Gus P. Coldebella

Deputy General Counsel

Office of the General CounselYes, these are correct. The only addition I can recommend (

[b5]

U.S. Department of Homeland Security

(b2) (office)

(b2) (mobile)

From: Isles, Adam [mailto: (b2)]
Sent: Thursday, December 07, 2006 6:30 PM
To: Levy, Andrew; Rosenzweig, Paul; Agen, Jarrod; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen; Spero, Deborah J; Ahern, Jayson P
Cc: Knocke, William R; (b2)
Subject: ACLU 514(e) Points

[b5]

(b2 b5)

2. Looping in CBP

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

(b2) tel

From: Levy, Andrew [mailto: (b2)]
Sent: Thursday, December 07, 2006 5:36 PM
To: Rosenzweig, Paul; Agen, Jarrod; Levy, Andrew; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen
Cc: Knocke, William R: (b6)
Subject: RE: ATS wash post question

Thoughts?

* * *

[b5]

(b2(2))

[b5]

Andrew J. Puglia Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

[b2] (work)

(cell)

(fax)

(b2)

(b2 b2)

(b6)

From: (b6)
Sent: Friday, December 08, 2006 10:01 AM
To: (b6)
Subject: FW: ACLU 514(e) Points

Attachments: ATS References.doc; ATS Article.doc

ATS ferences.doc (517 K

ATS Article.doc (41 KB)

(b6)
Senior Attorney
Office of Chief Counsel
U.S. Customs and Border Protection
Phone: [b2]
Fax:
email: (b2)

-----Original Message-----
From: (b6)
Sent: Friday, December 08, 2006 9:47 AM
To:
Cc: [b6]
Subject: FW: ACLU 514(e) Points

(b6)
Senior Attorney
Office of Chief Counsel
U.S. Customs and Border Protection
Phone: [b2]
Fax:
email: (b2)

-----Original Message-----
From: (b6)
Sent: Thursday, December 07, 2006 6:38 PM
To: (b6)
Cc: (b6) ROBLES, ALFONSO
Subject: FW: ACLU 514 (e) Points

(b6)

Since you will most likely be getting into the office early, please (b5)
(b5)

(b6)

(b6)
Deputy Chief Counsel
U.S. Customs and Border Protection
(b2)
ATTORNEY-CLIENT PRIVILEGED/ATTORNEY WORK PRODUCT

This communication might contain communications between attorney and client, communications that are part of the agency deliberative process, or attorney-work product, all of which are privileged and not subject to disclosure outside the agency or to the public. Please consult with the Office of Chief Counsel, U.S. Customs and Border Protection before disclosing any information contained in this email.

-----Original Message-----
From: (b6)
Sent: Thursday, December 07, 2006 9:05 PM
To: (b6)
Cc: ROBLES, ALFONSO; (b6)
Subject: FW: ACLU 514(e) Points

(b6)

[b5]

(b6)

(b6)
Deputy Chief Counsel
U.S. Customs and Border Protection
(b2)
ATTORNEY-CLIENT PRIVILEGED/ATTORNEY WORK PRODUCT

This communication might contain communications between attorney and client, communications that are part of the agency deliberative process, or attorney-work product, all of which are privileged and not subject to disclosure outside the agency or to the public. Please consult with the Office of Chief Counsel, U.S. Customs and Border Protection before disclosing any information contained in this email.

-----Original Message-----
From: SPERO, DEBORAH J
Sent: Thursday, December 07, 2006 8:27 PM
To: Isles, Adam; (b6) ; Isles, Adam
Cc: Levy, Andrew; Coldebella, Gus; (b6); ROBLES, ALFONSO;
(b2 & b6)

Subject: RE: ACLU 514(e) Points

As per my recent e-mail, the FY 07 report appropriated $27M. I am going to ask (b6) to provide the previous approps tomorrow.

-----Original Message-----
From: Isles, Adam [mailto:(b6)]
Sent: Thursday, December 07, 2006 8:15 PM
To: (b6) SPERO, DEBORAH J; Isles, Adam
Cc: Levy, Andrew; Coldebella, Gus
Subject: Re: ACLU 514(e) Points

Can we get those reports (tomorrow am)?

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: (b6) (b6)
To: Spero, Deborah J; Isles, Adam (b6)
Sent: Thu Dec 07 19:33:22 2006
Subject: FW: ACLU 514(e) Points

Sorry, I did not read you in earlier when I sent to Mr. Levy.

From: (b6)
Sent: Thursday, December 07, 2006 7:12 PM
To: Levy, Andrew; AHERN, JAYSON P; (b6 & b6)
(b6)
Subject: FW: ACLU 514(e) Points

Yes, these are correct. The only addition I can recommend (
[b5]

From:
[mailt [b6 & b6]
Sent: Thursday, December 07, 2006 6:34 PM
To: (b6)
Subject: Fw: ACLU 514(e) Points

Sent from my BlackBerry Handheld.

----- Original Message -----
From: "Coldebella, Gus" (b6)
Sent: 12/07/2006 06:29 PM
To: "Isles, Adam" (b6) ; "Levy, Andrew" (b6), "Rosenzweig, Paul" (b6) "Agen, Jarrod" (b6) ; "Coldebella, Gus" [b6] "Kraninger, Kathleen" ; "Spero, Deborah J" "Ahern, Jayson P" (b6)
Cc: "Knocke, William R" (b6) (b6) (b6).

Subject: RE: ACLU 514(e) Points

We're putting together more full talkers now-will include.

Gus P. Coldebella

Deputy General Counsel

Office of the General CounselYes, these are correct. The only addition I can recommend (

[b5]

U.S. Department of Homeland Security

(b6) (office)

(b6) (mobile)

From: Isles, Adam [mailto:(b6)
Sent: Thursday, December 07, 2006 6:30 PM
To: Levy, Andrew; Rosenzweig, Paul; Agen, Jarrod; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen; Spero, Deborah J; Ahern, Jayson P
Cc: Knocke, William R; (b6)
Subject: ACLU 514(e) Points

[b5]

2. Looping in CBP

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

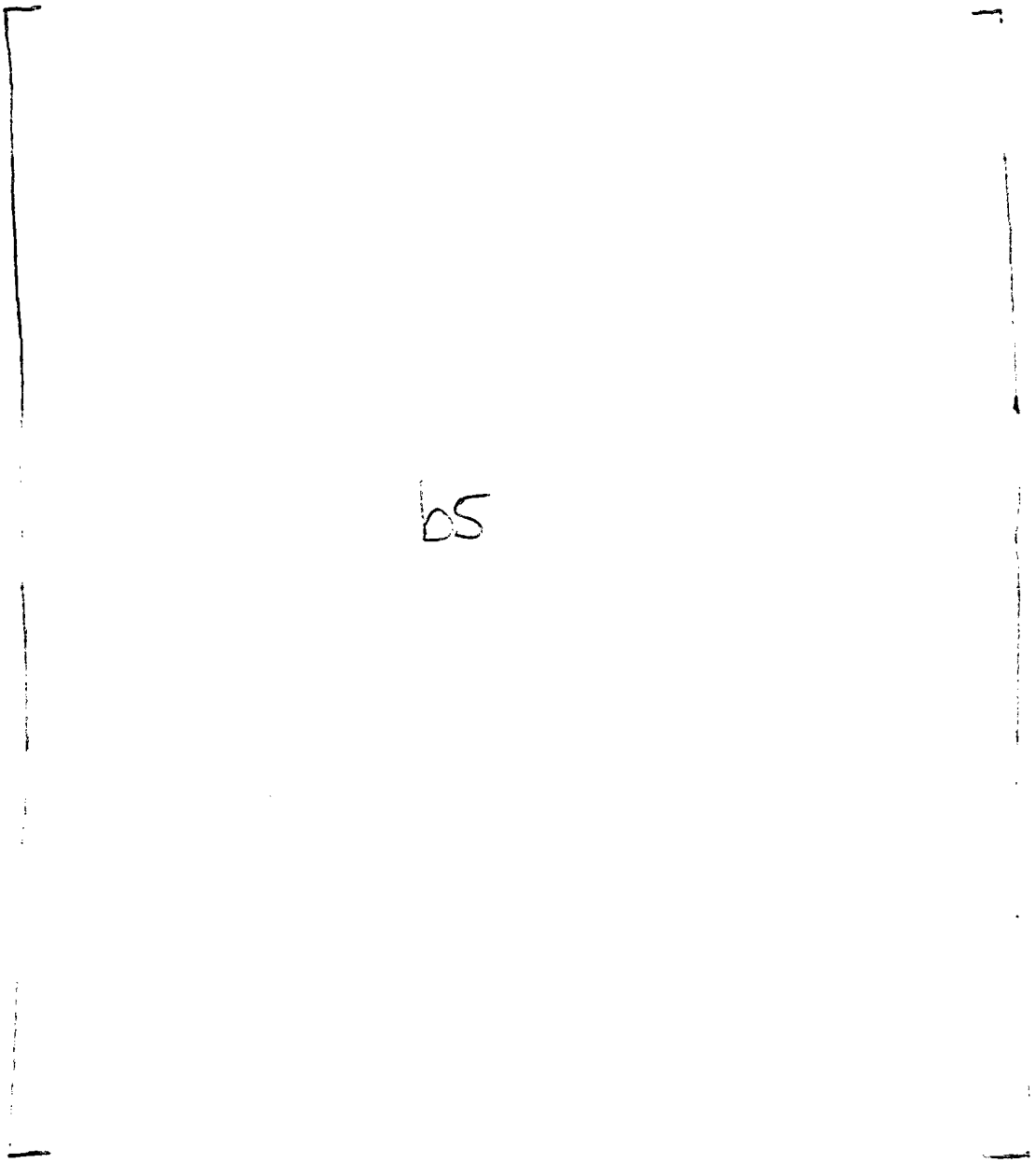
(b6) - tel

From: Levy, Andrew [mailto:(b6)
Sent: Thursday, December 07, 2006 5:36 PM
To: Rosenzweig, Paul; Agen, Jarrod; Levy, Andrew; Coldebella, Gus; Isles, Adam; Kraninger, Kathleen

Cc: Knocke, William R; (b6)
Subject: RE: ATS wash post question

Thoughts?

* * *



Andrew J. Puglia Levy

Associate General Counsel (Legal Counsel)

U.S. Department of Homeland Security

[b2] (work)

(cell)

(fax)

(b6)

From: SPERO, DEBORAH J
Sent: Thursday, December 07, 2006 8:25 PM
To: (b6) (b2 b6)
Subject: FW: AP: Traveler Risk System May Violate Ban

From: [b2 b6]
[mailto: [b2 b6]
Sent: Thursday, December 07, 2006 8:07 PM
To: (b2 b6) (b6)
Subject: Fw: AP: Traveler Risk System May Violate Ban

Fyi.

Sent from my BlackBerry Handheld.

----- Original Message -----
From: "Knocke, William R" (b2)
Sent: 12/07/2006 07:56 PM
To: "Jackson, Michael (DepSec)" (b2) (b6) (b2); "Sweet, Chad" (b2); "Perry, Phil" [b2]; "Coldebella, Gus" [b2] >; "Kent, Don" "Norton, James" < [b2] Baker, Stewart" (b2) >; "Ahern, Jayson P" (b2); "Rosenzweig, Paul" (b2); "Kraninger, Kathleen" (b2) >; "Isles, Adam" (b2)
Cc: "Agen, Jarrod" (b2); (b6) (b2) (b6) (b2); "Frawley, Anne Marie" (b2)
Subject: AP: Traveler Risk System May Violate Ban

Traveler Risk System May Violate Ban

By MICHAEL J. SNIFFEN
The Associated Press
Thursday, December 7, 2006; 7:47 PM

WASHINGTON -- The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years.

Some members of Congress and privacy advocates on Thursday questioned the legality of Automated Targeting System, or ATS, risk assessments that have been assigned to millions of Americans and foreigners who entered or left the United States over the past four years.

"It clearly goes contrary to what we have in law," Rep. Martin Sabo, D-Minn., said in an interview. He said ATS is the kind of computerized risk assessment "we have been trying to prohibit."

Homeland Security Secretary Michael Chertoff told The Associated Press: "I don't think it (the prohibition) can be read as applying to this program. The statute doesn't bar the use of funds for the purpose of analyzing the risks for people entering the country."

Department spokesman Russ Knocke said Congress was informed many times since 2003 that ATS was being used to assess people.

The AP reported last week that ATS has been assessing millions of people since 2002.

At that time, a law prompted by the attacks of Sept. 11, 2001, required air and cruise lines to give the Homeland Security Department advance data on all passengers and crew entering and leaving the country.

Jayson P. Ahern, assistant commissioner of customs and border protection, told the AP all that passenger data is analyzed by ATS. Data on rail and some land travelers also have been assessed, he said.

ATS has operated with little public notice or understanding until a description was published last month in the Federal Register, a fine print compendium of federal rules.

The Homeland Security Department's notice said people could not see their assessments or directly challenge them. It plans to keep the assessments for 40 years and share data with state, local and foreign governments for hiring, contracting, licensing and other decisions. In some instances, data could be shared with courts and private contractors.

Sabo, the top Democrat on the House Appropriations subcommittee on homeland security, wrote into the agency's spending bills the ban on computerized passenger risk assessments. For the past three budget years, the legislation has said no funds from the appropriations bill could be used to develop or test computerized data-mining tools "assigning risk to passengers whose names are not on government watch lists."

"They keep going off on these wild scenarios on a regular basis," Sabo said. "They should concentrate on making their watch lists comprehensive and correctable."

Sen. Patrick Leahy, a Vermont Democrat, agreed. "There is growing concern in Congress that this program invites abuse, and that the administration is plowing ahead with it in apparent violation of the law," said Leahy, a member of the counterpart subcommittee in the Senate and incoming chairman of the Senate Judiciary Committee.

Chertoff noted that the prohibition barred risk assessments of "passengers." He said "other people may have a different opinion of what they intended, but it's clear this is all aimed at what Secure Flight was, which was deciding who could board aircraft" in the United States.

Democrats and privacy advocates acknowledged the provision began in 2004 trying to prohibit computerized risk assessments using commercial databases by the proposed domestic screening system, then known as CAPPS II.

But they said when the agency changed the name to Secure Flight and dropped commercial databases, they broadened the prohibition in 2005. One section restricted Secure Flight only to testing and set accuracy and privacy tests before it could be implemented. But they said a separate section, covering the entire department, was added to prevent any use of computerized risk assessment of people who are not already on watch lists.

Knocke said the department provided written testimony about ATS to Congress 19 times since May 2003. Most of the written testimony contained a sentence or two saying ATS was being used to screen passengers. One statement specifically mentioned mining regulatory databases; one said ATS used computer algorithms to find potentially risky people for additional questioning at the border.

Ahern, the customs and border protection official, told the AP that ATS "is a very proven, forward-leaning border initiative that we put in place to try to take a look for people that basically weren't watch-listed."

Ahern said the ATS software finds people whose travel histories in the passenger records forwarded by air and cruise lines coincides with patterns of behavior that agents had seen among terrorists or criminals over time.

In comments filed with the government this week, The Identity Project, a legal defense fund for people whose travel has been impeded by government screening, argued ATS violated the spending ban and said "any records or data already collected ... for this forbidden purpose should be immediately destroyed."

The ban also was raised by Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty project; David Sobel, lawyer for the Electronic Frontier Foundation; and former Republican Rep. Bob Barr of Georgia, now a liberty and privacy expert for the American Conservative Union.

"We went through many years of debate over this notion of probing into the background of every passenger and assigning them a threat rating," Steinhardt said.

"Congress enacted a specific prohibition on rating innocent travelers and instructed DHS to focus only on those who were on a government watch list. So it is unconscionable for the government to then create this kind of a system in violation of that ban, and without proper notice to Congress or the public."

The department's operation of ATS since the ban was passed might violate the Anti-Deficiency Act, which bars government officials from spending money not appropriated by Congress, according to several of these critics.

That act carries administrative penalties that include firing. It also has criminal penalties for willful violations up to two years in prison, although no one ever has been prosecuted.

Russ Knocke
Press Secretary
Department of Homeland Security
Office [redacted]
Cell:
Fax:

(b6)

From: (b6 & b2)
Sent: Wednesday, December 13, 2006 12:45 PM
To: Levy, Andrew
Subject: Fw: EU press release on ATS/PNR

Some background on how we tried to address the pnr issues in the sorn and pia (b6)

----- Original Message -----
From: [redacted]
To: H[redacted] b2 & b6]
Cc: [redacted]
Sent: Wed Dec 13 12:16:00 2006
Subject: RE: EU press release on ATS/PNR

[redacted]

b5

[redacted]

(b2 b6)

[redacted]

[redacted]
Senior Attorney
Office of Chief Counsel
U.S. Customs and Border Protection
Phon[redacted]
Fax: [redacted]
email:[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday. December 13, 2006 11:59 AM

[redacted]

To: (b6)
Subject: Fw: EU press release on ATS/PNR

Adding ats gurus (b6)

----- Original Message -----
From: Isles, Adam [b2]
To: Agen, Jarrod [b2] ; Baker, Stewart ; White, Brian M ; Rosenzweig, Paul [b2] ; Isles, Adam [b2] ; Sales, Nathan (b2) ; Coldebella, Gus (b6) ; Levy, Andrew (b2) ; I(b6) (b2)
Cc: Knocke, William R <(b6) (b6) ; Kraninger, Kathleen (b6)
Sent: Wed Dec 13 11:54:13 2006
Subject: RE: EU press release on ATS/PNR

Looping in OGC too ...

Adam Isles

Counselor to the Secretary

U.S. Department of Homeland Security

(b6) - tel

From: Agen, Jarrod [mailto:(b6)
Sent: Wednesday, December 13, 2006 11:32 AM
To: Baker, Stewart; White, Brian M; Isles, Adam; Rosenzweig, Paul; Sales, Nathan
Cc: Knocke, William R; (b6) Kraninger, Kathleen
Subject: EU press release on ATS/PNR
Importance: High

EU pushed out this release today - getting several press calls here.

Given this is out of Frattini's office - do you have guidance on how you want me to push back?

Are we confident that ATS system is covered in Undertakings?

From: Strohm, Chris [mailto:CStrohm@nationaljournal.com]
Sent: Wednesday, December 13, 2006 11:42 AM
To: AGEN, JARROD; Knocke, William R
Subject: Seeking immediate comment for story
Importance: High

(b6)

Russ, Jarrod: I'm sorry for the short notice but I literally just got this. The EU today issued a statement on how PNR data is being used in the Automated Targeting System.

It says: "The information published by the DHS reveals significant differences between the way in which PNR data are handled within the Automated Targeting System on the one hand and the stricter regime for European PNR data according to the Undertakings given by the DHS."

The EU is sending DHS a letter asking for clarification and hints that this all could negatively affect renewal of the PNR agreement.

I'm doing a story on this for today. My deadline is 1:30pm. Again, sorry for the late notice but this literally just broke. Please email me or call me at 202-413-2212 with comment. The EU's full statement follows below. Chris

*****

This is a press release from the European Commission
Vice President Franco Frattini
European Commissioner responsible for Justice, Freedom and Security

"Data protection and transfer of PNR data"

European Parliament

Strasbourg, 13 December 2006

On 19th October the European Union and the United States concluded an agreement for the processing and transfer of passenger name record data by air carriers to the United States Department of Homeland Security. The US Government confirmed a set of Undertakings which guarantee the protection and security of PNR data.

Against this background concern has been expressed in recent days following information published last month by the Department of Homeland Security on the "Automated Targeting System". This is a security screening system making a risk assessment of international travellers relying, among other things, on PNR data. The information published by the DHS reveals significant differences between the way in which PNR data are handled within the Automated Targeting System on the one hand and the stricter regime for European PNR data according to the Undertakings given by the DHS.

The Council Presidency and Commission have sent today a letter to the US Government to request formal confirmation that the way EU PNR data are handled in the ATS is the one described in the Undertakings.

The current EU-US Agreement on PNR data will expire in July of next year. The Commission will, at the beginning of 2007, recommend to Council to mandate the Presidency, assisted by the Commission, to negotiate a new PNR agreement with the United States. I am sure that any new agreement will provide for a high level of data protection for all PNR data transferred under the agreement while protecting the security of our citizens.

I will keep the EP informed about the mandate and the progress of

(b)(6)

negotiations. COM expects to receive a mandate from Council before March next year.

I have always taken the position that travellers must be informed when their PNR data may be transferred to competent authorities of third countries. The DHS Undertakings expressly acknowledge this. We need an international agreement with the support of the public on both sides of the Atlantic and of the democratic representatives of the peoples.

I have often said that there is an important balance to be struck between measures to ensure security on the one hand and the protection of non-negotiable fundamental rights on the other. The Commission, assisting the Presidency in the negotiation of future PNR agreements with third countries, will ensure that security issues are properly addressed through the transfer and appropriate use of PNR data, while protecting personal data guaranteed by Article 8 of the Charter of Fundamental Rights.

Finally, a high level Contact Group was set up at the EU-US JLS Ministerial troika on 6 November 2006 to discuss information sharing and protection of personal data for law enforcement purposes. There is a clear need on both sides of the Atlantic to work more closely together on these issues.

I would personally be in favour of close contacts between the above High Level Group and both the European Parliament and the US Congress.

We need a broader perspective and a long-term vision to tackle, together with the US, the terrorist threat without putting at risk the fundamental rights of individuals.

I am also firmly committed to continue encouraging the Council to make progress on the Framework Decision on data protection in the Third Pillar. I hope the incoming German Presidency will be able to make substantial progress on that.

We do have a common problem and threat - terrorism - which will continue to exist in the coming months and years. Only a very solid strategy, and a balanced cooperation with our main international transatlantic partner, will allow reducing, if not eliminating, this modern form of 'totalitarianism' against democracy.

(1,2,3(1))

(b6) 08/31/01 10:57 AM
To:
cc: [b2 & b6]
Subject: Re: (b6) Variation #1 , aka : [b7E] examples

(b6)

It was my assumption from our discussion at the meeting that you needed (b7E) gained from any combination of factors, to have enough for a match of interest. When you introduced the two new factors, (b7E) you created the possibility of having (b7E) that are similar enough to get to (b7E) EVEN though the (b7E) are not the same, and the (b7E) are not the same.

What if tighten up the previous example a bit and we say:

[b7E]

are all present giving you over (b7E) Is this a match of any value?

Perhaps it should be not be called "cotravel", ([b7E] b7E)

I think you are saying this is not interesting. (b6) and (b6) may be indicating otherwise. My opinion doesn't matter!

(b6)

==========

(b6) 08/31/01 05:19 AM
cc: [b2 & b6]
Subject: Re[7]: (b7E) examples

(b6)

Am I correct in reading this info where there is no match on the first item? If I remember, there must be a match on the first item before anything else is considered. Since there is no match on the first item, then nothing else is to be considered.

(b6)

_____ Reply Separator _____ Subject: Re[6]: (b7E),
Author: (b2 & b6)
Date: 8/29/01 2:00 PM

(b6)

I AGREE!

(b6)

_____ Reply Separator _____ Subject: Re[5]: (b6)
Author: (b2 & b6 _)
Date: 08/29/2001 10:50 PM

(b6) I put the information into a table to make it easier to read. Based upon our discussions, YES, I do feel that this would be an valid example of a (b7E) situation. It would not necessarily be the case if you were missing the (b7E). In this case it appears that the (b7E) are sequential.

(b6) - any comments?

(b6)

==========

(b6) Is this a good match? : (b7E)

[b7E]

==========

(b6) 08/26/0111:18 AM
To: [b2 & b6]
cc:
Subject: Re[3]: (b7E) examples

Everyone,

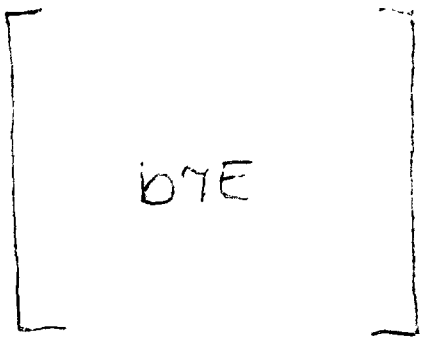
Here are some thoughts to consider.

[b7E]

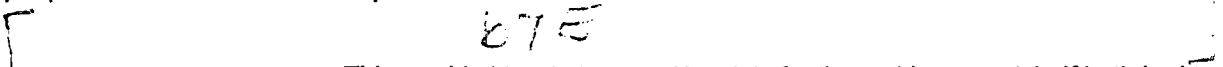
(b7E)

The point value will still be (b7E)

So here's what it would look like.



One of the main reasons for adding the (b7E) is because of the (b7E) program. If the subject qualifies for a (b7E), then there is no (b7E) This may help identify additional people. One issue that comes up is do we need to (



) This would at least give you 10 points for the residency match. If both had to match up, then you would receive no points.

Something to think about,

(b6)

_____ _____ Reply Separator _____ Subject: Re[2]: (b7E) examples
Author: (b6 , b7C)
Date: 8/19/01 8:32 PM

(b6)

I LOOKED AT THE EXAMPLES AND THE FIRST STATEMENT ON SLIDE ONE IS IN NEEDED OF ADJUSTMENT. (b7E)
(b7C)

THE SECOND STATEMENT MAY ALSO NEED TO HAVE SOMETHING ALONG THE LINE OF 10 POINTS. (b7E)
(b7E)

[b7E)

(b7E)

THESE ARE JUST SOME THOUGHTS BUT I BELIEVE THERE MAY BE OCCASIONS THAT THIS WOULD LEAD TO A NEED FOR SOME SORT OF ADDITIONAL WEIGHTING TO SET THESE MATCHES APART.

JUST SOME THOUGHTS, (b7C)

Reply Separator Subject:
Re: examples
Author:
Date: 08/19/2001 4:10 PM

I believe that when discussing the situation of Case 1, that we will want to have some score for the last element. I am thinking along the lines of 10 points. This will

please correct me if I am wrong. I believe that you brought this point up at the very end of the meeting on Wednesday

Reply Separator Subject:
examples
Author:
Date: 8/18/01 6:04 PM

Please review the examples contained in the attached powerpoint slides.

(b6).
02/18/2006 11:54 AM
To: (b6)
Cc:
Subject: Request for ATS-P3 Changes

(b6)

As per our earlier discussions, please forward the following requests for adjustments in of the ATS-P system to the appropriate OIT Managers:

[redacted]

b6
&
b7E

Please keep in mind that NTC Training Program will need to be revised to include any changes or updates in preparation for the new TDY group arriving in March.

Let me know if you have any questions or concerns.

(b6
National Targeting Center, CBP
Phone [redacted] b6
Direct
Fax

(b6)
03/03/2006 04:34 PM
To: (b6)
cc
Subject: Re: Start Page changes

-----Forwarded by (b6) on 03/03/2006 04:34PM -----

To: [redacted]
From: [redacted]
Date: 03/03/2006 04:19PM
Subject: Re: Start Page changes

we need to think outside the box on how to deliver this information the them but still clean up the start page. (

[redacted] b2 b5 & b7E

-----Forwarded by (b6) on 03/03/2006 04:17PM -----

To: (b6)
From: [redacted]
Date: 03/03/2006 03:08PM
Subject: Re: Start Page changes

[redacted] b2 b7E

With the constant TDY rotations and different ATS experience levels, it seems to be a valuable field for them as well.

(b6)
National Targeting Center
[redacted] b2

(b6)
03/06/2006 10:51 AM
To: [b6]
Cc: (b6)
Subject: Re: Start Page changes

Please see attached revision of ATS-P UR and FR. This includes comments from the NTC.

----- Forwarded by (b6) on 03/06/2006 10:49 AM -----
(b6)
03/02/2006 04:49 PM
To: [b2, & b6]
cc:
Subject: Re: Start Page changes

(b6)

Please see the ATS Startpage.doc for your review regarding changes to the Start Page. If you need any additional assistance, please feel free to contact (b6) or myself through one of the Watch Commanders. Thank you.

(b6)
National Targeting Center
(b2 ,)

----- (b6) wrote: -----

To:
From [b6]
Date: 02/28/2006 07:44PM
cc: (b2 & b6)
Subject: Re: Start Page changes

(b6)

Please review the attached ATS requirements document on Start Page changes and provide consolidated feedback to (b6) no later than Friday morning.

Thanks.

-(b6)

----- Forwarded by (b6) on 02/28/2006 07:41 PM -----
(b6)
02/28/2006 09:10 AM
To: (b6)
cc:
Subject: Start Page changes

(b6)

I apologize for sending these for review again but there is confusion because people at the NTC are speaking with the OIT programmers at the same time the personnel at the NTC are reviewing and commenting on User Requirements (the two processes are crossing and we are getting, at times, conflicting requirements). Please have whoever needs to review these requirements do so at their earliest convenience - as a lot of it benefits the NTC. After this I will finalize for implementation.

Thanks - (b6)

----- Forwarded by (b6) on 02/28/2006 09:07 AM -----
(b6)
02/24/2006 02:01 PM
To:
cc: [b2 & b6]
Subject: Start Page changes

(b6)

Here is the latest on the Start Page requirements. Please pass along to whomever you think needs to review.

[b2 high & b5]

I would request that everyone review the requirements that have already been implemented also in case those need to be updated/changed too. Maybe we can add them to the current development effort OR we may need to divide the requirements up into phases.

Thanks.

(b6)
Department of Homeland Security
Customs and Border Protection
P:
F: [b2]
(b2)

04/20/2006 06:34 PM
To:
cc:
Subject: Final Drafts of Requirements and Design Documents

for your review.
Powerpoint page 8: textbox should be (listed as
Powerpoint page 10:

Here are the final (?) draft of the requirements and design documents:

Please let me know if you have any comments (change tracking is enabled in the Word document).

Also, please let me know if they are satisfactory. If they are, I will transmit them "officially" to and request their certification.

Thanks.

b2 h, gh &
b7E

RISK SCORING & DATA SHARING
PROJECT TEAM CONTACT LIST
June 2005

b2 (low/high)

b6