

**CENTER FOR STRATEGIC AND  
INTERNATIONAL STUDIES (CSIS)**

**TERRORIST SCREENING AND PRIVACY ISSUES**

**SPEAKER:**

**THE HONORABLE STEWART A. BAKER,  
ASSISTANT SECRETARY FOR POLICY DEPARTMENT OF  
HOMELAND SECURITY**

**PANEL:**

**MARY DEROSA, SENIOR FELLOW,  
CSIS TECHNOLOGY AND PUBLIC POLICY PROGRAM**

**JIM HARPER,  
DIRECTOR, INFORMATION POLICY STUDIES, CATO  
INSTITUTE**

**SETH M.M. STODDER, ATTORNEY AT LAW,  
AKING GUMP STRAUSS HAUER & FELD LLP**

**MODERATOR:**

**DAVID HEYMAN,  
CSIS HOMELAND SECURITY PROGRAM**

**TUESDAY, DECEMBER 19, 2006**

*Transcript by:  
Federal News Service  
Washington, D.C.*

DAVID HEYMAN: Good morning, everyone. We're going to get started here. I'd like to welcome all of you to CSIS, the Center for Strategic and International Studies, in one of our ongoing discussions on homeland security strategy and policy. I'd also like to welcome our C-SPAN audience that are here joining us as well. Thank you all for tuning in.

CSIS, for those of you that are just joining us for the first time, is a non-profit, non-partisan Washington think tank, and for four decades we have been dedicated to providing the world leaders with insights on and solutions to some of the most challenging current and emerging global issues.

We're here today to discuss one of those issues: terrorist screening and privacy. This is one of the areas that was recommended by the 9/11 commission that we improve; that we find means and systems to ensure that the bad guys don't get in. Secretary Chertoff has said that, "Homeland security is really about risk, risk management. It's fundamental to managing the threat," he says, "while retaining our quality of life and living in freedom." He further says that, "Risk management must guide our decisions and we must examine how we can best organize to prevent, respond and recover from an attack."

So risk is coin of the realm. In homeland security, there are three primary things for risk for which we must be concerned of: keeping the bad guys out, keeping the bad things out and knowing what to protect and what level of security. It's a balancing act, all of this. We can never eliminate risk and we have limited resources. And, further, our national security interests extend beyond just national security per se in the nearer sense, but to our economic interests, our diplomatic interests and, of course, to our quality of life.

So we are here to talk about keeping the bad guys and the bad things out, and that's terrorist screening. How do we do this? How would you do this? How do protect against those who want to come in and do harm? What do we need to know? How do we know who is coming in and who's okay to come in?

We also want to respect, in this process, our fundamental rights. In 1974, the Privacy Act was passed by Congress, and I quote from it, saying that, "Each agency that maintains a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual."

At the heart of screening, however, there is a conflict. How much information do we contain? How much do we track? What do we do with it? What is its use? What is the redress if we think there is something wrong? And the system that is in discussion today that was developed over 10, 15 years ago, but now specifically to deal with

terrorism, is ATS: the Advanced Targeting System. And we'll hear more about that today.

Quite simply, though, it pulls together a number of different data elements, real time, for a number of different government systems and others, such as from commercial air travel, and we analyze that data – and I don't want to characterize it because I know the secretary will do a much a better job than I will. The question today, though, is do we have the right balance from risk and from protecting our quality of life. Do we have the right policy to assure that we reduce the risk of terrorism but also protect our rights and our economy?

Some have said that ATS is the most invasive system the government has yet deployed in terms of people affected. Others have said it provides the best means for keeping the bad guys and the bad stuff out. Who sets this policy? Who gives the best advice to the secretary to make the decisions on policy? Our speaker today – Stewart Baker, the assistant secretary for Policy – is the principal advisor to the secretary for Policy. He is the first assistant secretary and the longest-serving assistant secretary for Policy. His team must assess the risk, consider a number and national interests and advise what the best course of action is.

Assistant Secretary Baker was appointed by President Bush to be the assistant secretary in October 2005. Previously he served as general counsel of the National Security Agency. He has served as the deputy general counsel for the Department of Education. He has over 20 years of experience in government, but also in private practice and law issues. He was a law clerk to Judge John Paul Stevens and he has served, and been asked to serve, on numerous U.S. government private and international bodies dealing with national security technology and related policies. In 1994, he was awarded the Defense medal of Meritorious Civilian Service. He is a distinguished guest and we are honored to have him here.

Secretary Baker, thank you.

(Applause.)

STEWART BAKER: Thanks, David. It really is a pleasure to be here and I deeply appreciate CSIS's invitation to come address this issue.

I thought I would talk about three points and then we'll have an exchange among a group of panelists. First I want to talk about this program, the Automated Targeting System, and how it works, and then I'll address a couple of criticisms that have been leveled against it – first, the suggestion that somehow this was sneaked into law in the dead of night and then the suggestion that it's bad for privacy and civil liberties to have a program of this kind.

So those are the three points that I thought I would cover, but before I would do it, I'd like to begin with an event that's far from our borders. This is an event that occurred

in Iraq in February 2005, about 8:30 in the morning. A group of military and police recruits were gathered in front of a clinic, several hundred of them, and I think you can guess what happened next. You probably remember the headlines the next day. A young Jordanian drove into the crowd and set off a massive car bomb, killed a 125 people and wounded about the same number. The driver's name was Riyed Al-Bana (ph). We know that because the authorities actually found the steering wheel to the car that he blew up and his hand and forearm were still handcuffed to the steering wheel.

I'm not here to talk about what he did in 2005 but what he didn't do about 18 months earlier in 2003. That's when he showed up at O'Hare International Airport in Chicago with a valid passport from Jordan, a valid visa to come the United States to conduct business and he asked to be admitted. There's no bar to his being admitted other than the fact that he had been selected for a second look by our Automated Targeting System. He was flagged as somebody who just ought to be looked at more closely.

And so one of the CBP officers did exactly that: interviewed him, asked him a bunch of questions about what he intended to do in the United States, and concluded, at the end of the day, he just didn't like the answers. He wasn't confident that this guy was going to live up to the obligations that we imposed under the visa and he said, I'm sorry, you've got a valid visa, you've got a valid passport, you're not going to come into the United States, and he sent him back to Jordan. Eighteen months later, of course, he was in Hillah, Iraq driving the vehicle-borne IED.

So, no one knows what he was going to do in the United States, why he wanted to come in or what he was planning. Personally, I'm actually grateful that we don't know and that we didn't have a chance to find out because some CBP officer decided he didn't want to take a chance on letting him in based on the inquiries he had done using the information that he had available from our Automated Targeting System.

Next time we're not going to be so lucky, potentially, and that's because, suddenly, out of the blue, this program, which as been running for years and has protecting Americans for years, has become controversial. And there are people who say, well, that's an invasion of privacy; we need to abolish the program, restrict it, prevent it from being used to gather information that might be useful in questioning Americans. A variety of proposals for restricting that program have suddenly surfaced in the last month. I would say all of those proposals are bad ideas. This is a good program and it's a program that protects Americans by virtue of its operation.

Let me talk a little bit about how the program operates so you can see why I think that way. I'd like to start with the fact that hundreds of millions of people come to the United States every year; 87 million a year by air. It's a massive flow of people into the United States. DHS's job is to move those people smoothly through Immigration and Customs, to handle that flow of information, of people. That's not our first job, though. Our first job is to make sure that in that 87 million or that 400 million, if you're including the land borders, we're not admitting people who intend to do us harm.

So we've got about a minute, maybe two minutes that we spend with the average person coming into the country. That's all the time we have. If we tried to spend more than a minute or two with the air travelers that we saw, pretty quickly they would back up out into the tarmac.

So, how do we train our officers so that they can spot potential terrorists in a minute or two of interview and a look at their passport? Well, the answer is: you can't do that unless you're using extrasensory perception. The way we do that, the way we try to screen these passengers so that we have identified the most risky, is that we simply use that interview as a first screen to decide whether this is someone who needs a second look, who ought to go into our secondary processing and be interviewed in more depth about their plans and their reasons for coming to the United States.

So, how do we decide who gets a closer look? That's where the Automated Targeting System comes in. We've got information in the passport. We've got information from the questions, but the real value is the information that we've gathered in advance.

The way we gather this information is when people buy plane tickets they give the airline information that's needed for their reservation: their name, their passport numbers, frequent flier numbers, their credit card so that they can charge the account, a phone number when they can be reached. After the airline has gathered that information, DHS gathers the information from the airline and uses it to screen for potentially dangerous people. How do we do that? We look to see whether the name of the person who's coming in matches someone who's on a watch list for terrorism or a no fly list. So we first screen for the names of people that we're worried about.

We also do a quick link analysis. That is to say, we ask has this person given us information that establishes a link to a suspect address, say? Have they used an address that someone else who we actually believe might have been a terrorist has also used, or a phone number or a credit card number or a frequent flier number? And that allows us, if we find something like that, not to say, okay, this is a bad person, but this is someone we actually want to talk to for more than a minute or two.

This is a lesson – this search for these hidden links – maybe not so hidden links – is a lesson that we actually learned from September 11<sup>th</sup>. There were after-the-fact reviews of the hijackers' travel reservations in that case, and we found, from examining that information, that if we'd been able to explore all the links and all the ways in which those 19 hijackers were linked to people we knew about – knew were bad people – that we could have identified all of them, or virtually all of them, before the event. I'll walk through that for you.

We start with the two men we knew about. These are the men that flew American Airlines Flight 77 into the Pentagon: Al-Hamzi and Al-Midhar. We knew about them from intelligence. They had attended a terrorist gathering in Malaysia that was part of planning for the event and we put them on the watch list. They were already in the

country by the time we started looking for them. We didn't find them at the time because we discovered very late that we needed to be looking for them, but we at least were aware and, if we'd had more time and better information technology at the time, we probably could have located them.

If we had kept tugging on that thread, though, we wouldn't have just found them. We would have found other hijackers who used the same address as Al-Hamzi and Al-Midhar. I think we would have found three of them, including Atta, the ringleader of the plot. We could have found another hijacker because he used the same frequent flier number as the people that we had already identified.

And we're not done yet. Five other hijackers used the same phone number as Mohammed Atta. That's 11 of the 19 that we've found just by exploring simple links among the hijackers. And we could have found a 12<sup>th</sup> hijacker by looking at an INS watch list for people who had expired visas and we could have actually tracked down the remainder of them, not necessarily from their reservation data, but from other overlapping data between them and the people that we were investigating.

I think the fact that we didn't connect those dots, when we should have, is one of the great regrets that all of us about September 11. We don't know that it could have stopped the attack but it certainly is something that we should have done and we should have learned that lesson.

Now, we can connect those dots and the Automated Targeting System the way we do it. It allows us to look for those links among travelers, starting with someone we actually have strong suspicions about, and moving out to people that we haven't seen before that the terrorists are counting on us letting in because we haven't seen them.

Now, I wish that DHS could take full credit for having dreamed up this idea and having recommend it and having implemented it, but that's not the case. We're by no means the only people who believe that this system needed to be implemented.

Here's what the 9/11 Commission said about the importance of targeting travel. It said, "Targeting travel is at least as powerful a weapon against as terrorists as targeting their money. The United States should combine terrorist travel, intelligence operations and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators and constrain terrorist mobility."

And they didn't just say, oh, that's a great idea; do this; do something in the abstract. They had a very specific endorsement of exactly what we're doing here. They said, "The small terrorist travel intelligence collection and analysis program that's currently in place has produced disproportionately useful results. It should be expanded. Information systems able to detect potential terrorist indicators should be used at consulates, at primary border inspection lines, in immigration services offices and in intelligence and enforcement units."

It's hard to find a more specific recommendation in the commission's report. In fact, if we had not already built the Automated Targeting System, we could expect, with the legislation that Congress is planning to pass in the first 100 hours of the next Congress, would have required us to it. The reason Congress doesn't have to that in the next Congress is Congress has already done that. It's already authorized us to gather exactly the information that we're gathering for the Automated Targeting System.

This was just after the attacks of September 11th. Congress passed the Aviation and Transportation Security Act. It requires airlines to share reservation data about all U.S.-bound passengers with DHS. This is the information that goes into the Automated Targeting System.

Now, I suppose that if you really are imaginative, you could say, well, Congress told you to gather it. They didn't actually tell you to use it. Maybe you should put it in a box like the "Raiders of the Lost Ark" and, you know, have top men work on it someplace. But I don't think so. I think Congress intended us to actually dig into this and use it to try find people who we should put into secondary and interview to determine their intentions. And that's exactly what we're doing with it.

If there was any doubt about whether – sorry, I just wanted to let you know that we have moved into the second phase where I'm addressing the question of whether we sneaked this into law. And I think it's a little difficult to sneak, like, statutes into law. And Congress was very clear about the statute that they were enacting here and the importance of gathering this information. That's not all they did. Congress has funded this program. It has funded it as a line item for passenger screening, for several years, in the tens of millions of dollars. Congress knew exactly what it was authorizing and exactly what is was appropriating these funds for.

And, finally, I'd – talking about this issue, I want to stress how bipartisan the consensus in favor of this program has been up to this time. Obviously, the 9/11 Commission was an entirely bipartisan affair and the recommendation that we do this was unanimous. In addition, the 2001 Aviation Transportation Security Act that I talked about earlier passed with overwhelming Democratic support as well as Republican support. When it passed the Senate, we couldn't find any recorded dissents and when it passed the House it got 200 votes from the Democrats, as well as overwhelming support from Republicans.

In short, both parties, in several Congresses, have affirmed that we need to flag terrorists who may be coming into the United States and that we need to make passenger information available to DHS inspectors. It would be hard to imagine program that stands on firmer legal ground or that was better advertised than this program.

So, what's the basis for the opposition? Predictably, privacy groups have denounced it as unnecessary government surveillance program and as, I think David said, the worst or most comprehensive or intrusive, you know – the worst program this month, ever. (Laughter.) You know, I like to use lyrics from songs from the '80s when I give

speeches, and this one brings to mind the 1980s one-hit wonder Rockwell did: “Somebody’s watching me.” The refrain of which is “When I come home at night, bolt the door real tight. People call me on the phone I’m trying to avoid. Can the people on TV see me or am I just paranoid?”

Now, we know from tee shirts if nothing else that even paranoids have enemies, but I think there’s a corollary to that which is that sometimes paranoids are just paranoid. And I think in this case, that’s exactly what’s going on. The Automated Targeting System is not a threat to privacy. It’s not exactly a dossier, to start, of our most intimate secrets. This is travel reservation data. You gave it to the travel agent. You gave it to the airline. They’re going to give to the guys who load the plane, set up the meals, who assign the seats. This is information that is going to be used widely in order to make the trip a little more convenient for the traveler.

So, if the airlines are using it just to make the trip more convenient, I have to ask: Who’s going to object to the idea that we ought to actually use it to make sure that the plane arrives safely at its destination and that the travelers, when they get into the United States, are safe from terrorist attack? That’s the purpose of the program and that seems to me, not only is this information, not particularly sensitive, but has enormous value in preventing terrorism.

I also want to stress how much effort we put into making sure that the information is not abused. If anyone who wants access to this information – any DHS employee wants access to this information – they have to pass a background check, they have to maintain a security clearance. Even though the data is not classified, it is information that we want to have similar kinds of background checks for people to gain access to.

Supervisors – only supervisors – have access to certain particularly sensitive bits of information and everybody who uses this system is audited. Every system inquiry is logged. It can be traced back to the employee who made the search. We have no tolerance for abuses of the system by the employees. When we find some misuse of this system, we can be very tough on people. Employees who break the rules face penalties that range from suspension to termination and we’re not unwilling to use all of those disciplinary measures.

And finally, as I said earlier, you have to look also on the other side of the equation. Let’s suppose that privacy advocates got their way and we shut the program down. How exactly would they propose we’re going to protect ourselves from terrorism? Now, there’s a limited number of tools that you have when you’re trying to address the problem of terrorism. We’ve got to make everybody go through a screening system in which everybody takes off their shoes, everybody puts their luggage through, everybody walks through the magnetometer. And the privacy advocates say, well, that’s silly. You’re putting grandmothers and infants through those things when they’re obviously not a threat. Why are you making all of us go through this when you’re really only looking for a few people?

So maybe we should select people based on some characteristics. Well, if we only have a minute or two to make that decision, how good is our decision going to be? Are we supposed to be making this on the basis of how people look, on the basis of one or two questions, on the basis of just of our intuition? I think the response of the advocates is, no, that's going to encourage profiling and discrimination, and you can't do that. So the answer is, let's go get more information so we're making a better, more individualized judgment about who we screen for and who gets special attention. And as soon as we do that, the cry is, well, now you're building a giant database. You can't do that.

You have to ask yourself, what's left to protect against terrorism? Are we supposed to pray? Well, not in a public building, I understand. (Laughter.) This is by far our best, most sensitive tool for making decisions that are not discriminatory and that are based on actual data rather than guesses about people's behavior.

Let me close by just talking a little bit more about the value of the program by examining some of the other circumstances in which it's been used – just a couple of stories.

Al-Bhana (ph) not the only person that ATS has helped keep out of the country. Every day we find value in this information. We make decisions not to allow someone into the country because of information that we were able to glean, starting with what is provided by the automated targeting system.

Just a few months ago in Minneapolis-St. Paul the automated targeting system flagged a high-risk traveler for additional scrutiny. We put him in the secondary screening and began talking to him. Once we had him there we looked through his luggage and we found a manual on how to make improvised explosive devices, IEDs, the kind of bombs that terrorists have used in Iraq and Afghanistan to attack U.S. troops with.

We also found video clips of exactly that kind of attack using IEDs to kill soldiers and destroy vehicles, as well as a video on martyrdom. This is a very dangerous guy. We found him because he was originally flagged for an interview, and when we went through the interview and began looking at him more closely, we found more and more reason to be worried. That's exactly how this system should work and how it does work.

It's not just terrorists that we can find by doing this kind of examination of people's travel patterns. We can also break up international criminal activity. In March of 2004, a woman came through Newark Airport from the Dominican Republic, and she was accompanied by her children. She had their birth certificates. The data all seemed to match up. But when our officers started looking closely at her travel pattern in the automated targeting system, they noticed that she hadn't taken her kids with her when she left. In fact, she had several trips where she left without them and came back with them. She was smuggling kids in using kids whose ages approximated those that she had birth certificates for.

We went further. We said, well, who has traveled with this woman – made reservations with her or traveled with her in the past? It turns out they were all leaving without their kids and coming back with them. We actually broke up an entire ring of child smugglers just by using this kind of information.

So in conclusion, let me just remind everyone that our border is our last, best chance to identify and turn away terrorists. Once they're in the country, they're much harder to find, they're much harder to stop. We need the best possible information about the hundreds of millions of people who cross our borders every year if we're going to have an effective program to stop terrorists at the border. The automated targeting system helps us marshal that information. It helps us protect Americans from terrorism. And the more that people learn about this program – including people in Congress – the more I'm confident that they will support it, and if possible, expand it. Thank you.

(Applause.)

MR. HEYMAN: Thank you, Mr. Secretary.

Our second half of the program will be a panel discussion. I'd like to invite our panelists up right now. We will have a discussion with the secretary, and I'd like to invite up Mary DeRosa, Jim Harper and Seth Stodder, some of the leading thinkers on these types of issues. Particularly they're going to balance the questions of privacy and national security issues.

Mary DeRosa, here at the center, was a special assistant to the president of the National Security Council during the Clinton administration. She has served on a number of commissions, and also in private practice.

Jim Harper is the current director of the Information Policy Studies at the Cato Institute, also working on a number of these difficult problems of adapting law and policy to the unique problems of the information age. He also serves as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Seth Stodder, senior counsel at Akin Gump, served in the Department of Homeland Security after its creation, in the direction of Policy and Planning for Customs and Borders. He currently, as I said, is at Akin Gump and working on appellate and constitutional litigation matters.

What I'd like to do is ask each of the panelists to maybe offer a few observations and considerations about the issue, and then we'll have a discussion with the secretary, and if we have a little time left we'll bring in the folks in the audience.

Seth, do you want to start?

SETH STODDER: Sure. Can everybody hear me? I don't want to reiterate too much what Secretary Baker has very eloquently said, but I think – I mean, a couple of

things. I think a lot of the flap over the ATS issue may have started, I think, from some confusion with regard to the difference between screening passengers for domestic aviation purposes to protect airplanes versus screening people for admissibility into the United States on our border. And I think there is a crucial difference there.

Primarily – I mean, I'm a lawyer so I'm going to start with the law. One of the issues of law to think about here is that under Title 8 of the United States code, the Immigration and Nationality Act, CBP officers have the absolute authority to ask questions of anybody coming into the United States of any nature, probative of admissibility, and can also search any person or thing or luggage to determine admissibility.

Over and above that, CBP officers from legacy customs authorities – custom border search authority – have the absolute right to, with some limited exceptions, to search things, luggage, to determine whether bad things or inadmissible things – things are coming into the country. And all of this is done and can be done without a warrant, without probable cause, without reasonable suspicion, for the most part.

So that's really sort of the basic framework, legal framework, to start with when you think about the automated targeting system. So all of the information that you could see within the automated targeting system, whether it be credit card information that you purchase your flight, frequent flyer information, all that – all of those data elements that are provided to, say, the reservation companies, or is provided as part of the feed from the airlines as part of the advanced passenger information feeds, all of those data elements could be asked of you and any single person seeking admission into the United States by a CBP officer at primary or at secondary. And that would be anybody in the sense that because under the immigration code of the Immigration Nationality Act, the burden of proving admissibility into the United States is on the applicant for admission. The burden is not on the government to show inadmissibility; the burden is on the applicant to show admissibility.

So therefore, there really is no privacy issue per se because all of the data elements that could conceivably be at issue with regard to ATS could be asked of you when you come to the country – come to a port of entry.

So, now, it could be – now, as Secretary Baker mentioned, 87 million people come into international airports every year. Over 300 million further come in through land border ports of entry. Now, you could envision a system where you could ask all of the questions that would be data elements within ATS of each person at primer. And as Secretary Baker indicated, you would have planes backed up all the way to Halifax, or wherever they're going to be backed away to.

So the airlines actually – this is not the government – actually the airlines, in the 1980s, pushed customs and the INS and worked together to create a system of gaining advance information. And this was a voluntary system where the airlines actually provided this information. And when we think about advance information, we need to

think about two difference tranches of information. One is advanced passenger information, which is basically your passport and visa data, that is pushed to the government by the airlines when you check in for your plane. And the other tranche of data is passenger name record information – it’s a PNR, which Secretary Baker indicated. It’s your reservation data that, when you make a reservation, the information that’s within there is within the PNR data.

And the airlines worked with customs and the INS to pull together a system whereby the government could obtain this information and screen people and try to narrow the range of questions that they would need to ask at primary – to do what? To ensure security and ensure against illegal immigration and illegal smuggling, but also to facilitate the movement of people through airports. That was the point of the system. And now, along the way, we realize, wow, this has an enormous security benefit, not only for the ability to check watch lists, but also the ability to do the kind of link analysis that Secretary Baker indicated. And so Congress said, after 9/11, and the 9/11 Commission said, gee, that’s a good idea. Congress enacted the ATSA and mandated by law that the airlines provide this information, and has continually reauthorized this program.

So, I don’t want to filibuster too much, but I think that the key thing to sort of think about here is to make the distinction between what you would do internally with regard to domestic passenger aviation, the kind of information that you might see under a CAPS 2-type program or a Secure Flight-type program, and the limitations, the Constitutional limitations, you might see versus what you do at the border with the ATS system where, under the law, CPB can ask any question it wants of you to determine inadmissibility.

And by the way, what are grounds of inadmissibility? Just final point here. Grounds of inadmissibility is not just seeking illegal immigration, but being a terrorist is a ground for inadmissibility. Bringing in false documents is a ground of inadmissibility. Fraud is a ground of inadmissibility.

So you could ask a question, say, did you use the same credit card as Mohamed Atta? That would be a question that you could ask, but if you could determine that through the ATS system beforehand, it might be helpful.

MR. HEYMAN: Thank you, Seth.

Why don’t we keep moving down the line? Jim, would you like to address a couple of issues and put them on the table for discussion? Thank you.

JIM HARPER: I think, unlike screening for terrorists at the border, Secretary Baker provided me with a target-rich environment in his talk just now.

The story of the suicide bomber in Iraq was gripping and thrilling, frankly, but I think it was an invitation to us to indulge in what’s known as the post hoc ergo propter hoc fallacy. That’s Latin for “because it followed in time, there must be correlation.”

Because ATS existed, he was stopped at the border. It may be true, but not necessarily true. Had he gotten into the country, he would have done in this country what he was able to do in Iraq. Maybe true, but probably not true. The infrastructure isn't here and the support isn't here to be able to pull off that kind of thing. So it's, again, a gripping story, but not necessarily a good basis for policymaking.

In addressing what ATS is, it's a check against the no-fly list. I think most people are aware of that. Link analysis, it makes pretty good sense in many cases. Didn't address the question of the risk score, which is the most concerning, I think, to most people, for a variety of reasons. And exactly how that risk score is created isn't known, and I imagine that Secretary Baker and others would refuse to tell us how that risk score is created because that would create a security breach in the system.

But it's precisely there that the capacity for rank unfairness in the system is created. And it's a system that doesn't just apply, as I understand it, to foreigners coming to the country, but to everyone traversing the border, and that's – I'm sorry to be so parochial, but I'm most interested in the rights of American citizens who are traveling internationally and returning to the country.

A couple of – next in our logical fallacies lesson, Stewart used a few examples of straw man argument. The question of whether ATS was snuck into law in toto I don't think has been raised by anyone. I haven't seen it raised by anyone. But the scope and extent of it may have been – and in fact it was operating without a Privacy Act notice, as required by law until just a couple of weeks ago. I can understand how that happens – folks building a program or doing – imagine they're doing wonderful things and may be doing wonderful things, and someone turns around at some point, some lawyer, says, hey, there is no Privacy Act notice for this. You've migrated the program to where one is needed, and now it's needed.

So we didn't have the public disclosure of what was going on in advance, maybe because you don't publicly disclose in advance what you're just evolving naturally to do in addition to privacy impact assessment. Those only were just issued and came to light.

So there isn't a wholesale allegation that the entire program is ultra vires or contrary to law; it's just that many of the laws that require disclosure of this thing so we can have this kind of public consideration hadn't been followed up to this point.

There is the open question of appropriations language in the 2007 Appropriations Act that says there shall be a – and I paraphrase, perhaps badly – there shall be no risk scoring as to people who are not on a no-fly list. The argument is that that applies only to the Secure Flight program, but I think you have to pretzel yourself a little bit to get around the very clear language in the appropriations law.

I guess I won't go too long because there are a lot of things to discuss, but I don't think the folks who are advocating for privacy and transparency in this program are arguing for it to be shut down or for the elements that work to be shut down. It's

obviously a much more granular argument than that and I don't think it's necessarily fair to say that privacy activists are trying to shut down ATS. Privacy activists are pushing, just like all kinds of interests are pushing, to make sure that we get security programs that work, and we stay away from security programs that are premised on mass surveillance, denial of due process, and things that I think are pretty basic to what this country is all about.

I endorse the "Chertoff-Heyman doctrine" of risk management, and in the DHS Privacy Committee we issued a framework document – a framework for our own use in consideration of programs, technologies and so on and so forth, and job one is to determine how the program technology, or whatever you're looking addresses a risk and how well it addresses that risk. And I have – despite the existence of wonderful anecdotes, I have real concerns that identity-based security works very well because there are so many ways to evade it, among them physically evading it; that is, coming into the country outside of any controlled border. Then logical evasion of a variety of types. That is false documentation. We can work to improve that. That is coming to the country without having a history of bad behavior. That's what the 9/11 terrorists did so capably, and al Qaeda. Then there is the extremely fiendish technique of being born inside the country, which is what Timothy McVeigh did in order to evade our border security and carry out his attacks. I say this somewhat in jest, but it's very last battle to secure our borders when the next terrorist attack could come domestically.

The better approach than to do identity, to figure out who everyone is and what they're all about and what they plan; better than that wonderful intellectual experiment is to secure our infrastructure against the tools and methods of attack that anyone might use – that anyone might use, no matter their motivation, their background or anything else. Securing cockpit doors is an example of precisely that, and the commandeering attack against airlines is effectively foreclosed by that simple procedure.

MR. HEYMAN: Thank you, Jim.

We'll have one more commentary and then we'll have a discussion from the secretary. Mary?

MARY DEROSA: Thank you. In general, I am not willing to write off automated data analysis types of programs. I think that these can be very powerful tools, and I don't think they're tools that we should take off the table. But I do think that they are tools that can be used in a way that is unduly intrusive. And so you need to, when looking at a program such as this one, be very careful. They can be done in a way that protects privacy; they can be done in a way that doesn't.

And I was very interested to hear some more information about the program from Stewart. There are generally five questions that I ask when I look at a program that uses an automated data analysis, sometimes called data mining, but that's a very inexact term. The first question is what is the purpose or mission of the analysis? The broader or less clear the purpose or the mission, then the more likely you are to have an ineffective and

inaccurate analysis. And I'll sort of tick through these and then maybe quickly apply them to raise some questions about this program.

The second question I like to ask: What type of analysis is it? And this is where the definition of data mining – there are all sorts of different ways that you can do automated analysis. Some of them start with individualized suspicion, start with a subject, and analyze from there. Some of them look for a pattern. I think generally speaking if you're doing a pattern-based analysis, that raises far greater concerns because it isn't the kind of – it's more like profiling. It is not based on an individualized suspicion, which is generally a type of analysis that investigations were more typically used.

The third question: How accurate is the analysis, and how do you know? How do you know whether you are getting 1 percent false positives or 95 percent false positives? It's a critical question and one that you always will want to know the answer to.

Question number four: How are the results of the analysis going to be used? And there are different ways to use them that raise far different questions. If the results of a pattern analysis are used to deprive somebody, based solely on that analysis, of a liberty, then much more of a problem than if they are being used to be – just information to be used for further investigation.

And finally, how well is privacy controlled and overseen in the use of this analysis? What kinds of protections are there on use of the data, retention of the data? What kind of guidelines? How often are they audited?

So very quickly, when I looked over the privacy impact assessment for this program, I had some questions: first, purpose or mission. The mission is described not only as a terrorist – to catch terrorists, but also sort of generally bad guys, criminals. That to me raises some questions about how are you – this isn't very – it's kind of broad and I think less likely to be accurate if there are definitely different considerations that go into catching terrorists and catching all other kinds of bad guys, and so that raised a concern for me.

The type of analysis wasn't clear to me. Risk assessment – as Jim pointed out, risk assessment figure implied to me some sort of a pattern, but you described a link analysis, which is more of a subject-based analysis. So if that is – if it really is more link analysis than a pattern-base assessment that raises less of a concern. But link analysis or pattern based accuracy is still a major consideration and obviously we can't know what the model is or what the analysis is, but I would be very interested in knowing what kind of testing there is done for the accuracy of this program because – and how accurate it is, and how do you know, and do you know how accurate – do you know how many perfectly innocent people are being pulled in every time for every person who really does raise concerns.

How will the results be used? On this I have less of a concern if in fact the results are used only to put somebody over to secondary screening. That to me doesn't seem like that significant of a burden on that score, unless there is, again, something I don't know. That is less troubling. But what is more troubling for me is on the final category of protections and control, the retention period for the information in this program is 40 years. I can't imagine a reason why you would need to keep this information and these risk assessments for 40 years. The explanation in the PIA is this is related to what is thought to be the sort of working life of the terrorist or criminal, but I think that is something that really should get some more analysis because 40 years retention on this data seems – and David is looking at me like you'd like me to move on.

So basically – and redress is another issue that causes me significant concerns. So I'll stop there.

MR. HEYMAN: Thank you.

For those of you who are not in Washington, PIA is a privacy impact assessment.

MS. DEROSA: I think I said that.

MR. HEYMAN: I just want to make sure everyone is paying attention out there.

If I may summarize – there is a lot of questions and comments you gave out, and you obviously can respond to any of them. There is four key ones that I hear that I would like to – if maybe I could summarize them that I think people would be interested in your comments on. Number one, Jim talks about rank unfairness and the denial of due process, a great concern about that. Mary talks about redress. So maybe if you could talk about if people feel that they have been harmed in some way, what is the process for redress in that situation?

Two, the question of the risk score. I actually do think that we should keep what we're looking for kind of secret because otherwise people can avoid that. But it gets to the question of redress. If you think that you're being unfairly targeted, how can you deal with that? And so maybe you could comment a little bit on the risks for – third, Mary makes the point about 40 years – a lot of people have talked about that. They don't understand perhaps why the data is being held for so long. And it gets to the question of use. Will there be some use downstream that I have to worry about as an individual that I'm not prepared to know about today that some future administration may choose to use this for?

And finally, the question of – and also I guess related to the personal investment of individuals in this system, and that is, when can I have access to my own records just to check it out. Even if there is a redress system, does it include my ability to look and make my own judgments? So perhaps those four categories, redress, risks for 40 years, and access to our own records. Thank you.

MR. BAKER: Okay, is that all?

MR. HEYMAN: And we have 30 seconds. (Laughter.)

MR. BAKER: Yeah, let me see if I can take these in order. I thought the most significant thing that was said, putting aside Seth's remarks, which I completely agreed with, was Mary's suggestion that if the worst that happens is that you go into secondary, it's not such a big deal. But that is how this works. This is a screening device that is used to put people into secondary. Now, you may get asked questions about the information that we have in the automated targeting system at that point.

I'm thinking actually that we're going to recommend renaming secondary. We are going to call it our redress procedure because if in fact the information that we have is wrong, you should just say that actually that is not right; I didn't go to Pakistan for those years; you must have somebody else's record. So you just have to answer questions. If you answer them in a way that leaves people doubting your truthfulness, then they can take that into account in deciding if you're not an American whether to admit you to the country, but since this system is used simply to put people into secondary and ask them questions, the way in which you can correct the information is pretty straightforward.

By and large, apart from information that is generated by the government itself, this is information that is either on somebody's passport, or it's in the travel reservations that they made, and those are records that are pretty well within your control and something that you can examine. If somebody wants to know what information is there about me in this system, we actually do allow people to file FOIA, Freedom of Information Act requests to find out information about themselves, not about other people. So there is a way to find out what information is stored in the system, but it's very rarely used because the information is so anodyne.

The retention period, we haven't kept information for 40 years. We have kept it for about five because that is when we really started gathering it in substantial amounts after the 2001 Act. The standard for law enforcement information where you want to carry out an investigation and make sure that you can go back and see if you missed something in your first criminal investigation is 40 years. And I have to say, you know, we're dealing with people who had a 13-year gap between the first attack on the World Trade Center and the second attack on the World Trade Center. The idea that you would say, oh, well, we can get rid of this data in 10 years strikes me as pretty irresponsible.

So we have got plenty of time to decide whether 30 or 40 years is the right time, right period to keep this data for. And if you all want to come back and debate that in 2030, you can do it without me.

I think that the last issue that I just wanted to mention – Jim raised a lot of good points, some of them so deep inside the Beltway but I'm not sure we want to raise them here. But he said he was really worried about the rights of Americans, but the best way to evade our border controls was to be an American. That is precisely the problem.

We're not a country that are free of people who want to commit terrorist acts. No country is. Many of the people that we are most concerned about from a terrorism point of view who cross our borders are American. The idea that we would say, oh, you have got a free pass; we don't get to ask you questions; we don't get to see that you went to Pakistan and spent six months there without a job and ask about that, it's crazy. We have to be able to ask that information from people crossing the border, whether they are from France or the United States.

So I'll stop there. If I have left anything out, let me know. Oh, risk scores, yeah. Where did this come from? I don't think there is a risk score.

MS. DEROSA: It's in the privacy impact.

MR. BAKER: We do do an assessment of people when we look at the data, but that could vary from flight to flight, day to day. We might say we have intelligence that somebody is targeting a flight from Amsterdam to the United States or flights from Amsterdam, then we would say let's put special care, let's look closely at folks from – flights from Amsterdam. I think the risk score may reflect the fact that this system also may be used, or some parts of the system are used for cargo. We have a risk source for cargo, and we give a whole bunch of factors that say this particular shipment from somebody we never heard of to somebody we never heard of, using a fly-by-night carrier, yeah, we're more – that is going to get a higher score and more likely to get looked at than one more shipment of sneakers to Wal-Mart. But I don't think that we're scoring human beings, and we're certainly not keeping score on them, so there is nothing to disclose there.

MS. DEROSA: Well, I would just say that in the privacy impact assessment, it does talk about risk scores, risk assessments, and those scores are kept for the – the retention period on that assessment is 40 years, which is, if you're saying – I read it to mean that those risk scores on people –

MR. BAKER: No.

MS. DEROSA: If you are saying that they are not, then that is certainly something that – it's comforting. It's not clear from the PIA, however.

MR. BAKER: I'll note in addition that the CBP website, one web page among many I'm sure, identify ATS as a data mining system, data mining program. Now, there is plenty of wiggle room for what that means, but there is a lot of evidence out there that weird stuff is happening.

MR. HEYMAN: Let me jump in here. We have very little time because the secretary has to go. I'm going to ask – if the reporters here to – we are going to take two questions, one after the other, and then we'll – you can answer them, and then we have a little time outside that people can take that. So right here.

Q: (Off mike.)

MR. HEYMAN: Take the mike please.

Q: Sorry. We spoke about two weeks ago about a study that you did saying that data mining, especially the government program right now, is about 90 percent ineffective. I was just wondering if Mr. Baker could speak to that.

MR. HEYMAN: Okay, hold the answer. Let's just get a couple of more.

Q: Mr. Baker, I just want to ask you –

MR. HEYMAN: Could you identify yourself for the audience, please?

Q: Yes, Wilson Dizard with Government Computer News. I wanted to ask you, with regard to improving, or even really fully disclosing the privacy aspects of this system, and in the knowledge that the overall U.S. visit, network of networks potentially is linked to others that allow federated searches of across dozens and dozens of databases, what do you think of the possibility of actually just going head and using technical methods to improve the privacy by using, say, for example, anonymizing techniques so you can look into the databases without actually grabbing out all of the data, or other methods of, say, for example, looking at how the intelligence community is going to consolidate its data protection levels, and raising or assuring the American public that, even your own employees that their personal data protection, which might be one of the 100 laptops lost at Dulles every day, is in fact protected at a secure level.

MR. HEYMAN: Okay, let me jump in here. One last question and then we'll –

Q: Peter Swire, Center for American Progress. Stewart, when you were in the private sector before you came into government, you wrote an article about anonymizing techniques and how that could be used with Europe for PNRs, and we'll talk about PNRs today. Do you still agree with what you wrote then, or if not, has something changed? (Laughter.)

MR. HEYMAN: Okay, if you want to just take those last three questions.

MR. BAKER: I really have stopped beating my wife. (Laughter.) Let me – I'll deal with that quickly. I don't think there is anything in that article that is inconsistent with what I hear here. And to tie it into the earlier question that can we use technology to improve security and privacy? Absolutely. I think fighting technology is dumb. We're not going to be able to put data back in the box. We can't un-invent Google. Data is going to be more widely available in general. But we can use those same tools to make it harder for people to abuse the information, and one of the things we do is use audit tools to make sure we know all of the searches that our officers or anybody who has access to this data are performing.

And so we can look for abusive searches, and we have mechanisms for search to identify abusive searches, as well as random audits, and that is precisely the kind of thing that is an effective privacy protection in the 21<sup>st</sup> century.

Finally, let me just deal with data mining. I think that is sort of the equivalent of an ethnic slur for using information to find people that you're worried about. We do use information to find people that we're worried about. We look for names of terrorists that were – that we have on the watch list. We have look for links to known terrorists or known terrorist locations, and if we can, we would be glad to look for patterns that establish reason to ask questions.

I think, you know, if you take five trips to the Dominican Republic and you take your kids every time, and you never bring them back, that is a pattern we ought to ask that person about. It doesn't seem to me that calling up data mining ought to change the fact that we ought to be looking at people like that. Thanks.

MR. HEYMAN: Well, this is going to – let's wrap it up here. First of all, this is a challenge for Americans as they wrestle with these new technologies, new security environment. And there is – everyone desires to be safe, to be secure, to be able to maintain their commerce and their freedoms, and the challenges will be continued. I think these discussions help that in terms of bringing transparency and understanding of the difficult new issues. I want to thank you, Mr. Secretary, Mary DeRosa, Jim, Seth, thank all of you for this discussion; look forward to more of them in the future.

(Applause.)

(END)