TSA Oversight Part I: Whole Body Imaging

Statement of Stewart A. Baker
Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security

Before the Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense, and Foreign Operations
U.S. House of Representatives

March 16, 2011

Chairman Chaffetz and Ranking Member Tierney, I appreciate the opportunity to provide this statement today. The Transportation Security Administration's use of Advanced Technology Imaging, and TSA's broader efforts to secure passenger flights against terrorists, are important topics about which I have been outspoken. Much of what I will say today is consistent with things I have said before – as the head of the Department of Homeland Security's policy shop in the previous administration, in a book that I wrote soon after the Bush administration ended, and most recently in articles, blog posts, and interviews. I should note at the outset that while I maintain an active homeland security law practice, I am not representing companies selling Advanced Imaging Technology to TSA.

The Threat Is Real

Let me start with a point that should be obvious but sometimes gets lost: the threat is real. Terrorists – specifically al Qaeda and its affiliates – are trying to blow up planes flying in and to the United States. They tried to do it with Richard Reid, the shoebomber, back in December 2001. We were fortunate that the explosive in his shoe did not detonate. They tried to do it with the liquid explosives plot to bring down 10 airliners in the summer of 2006. We were fortunate that British and U.S. law enforcement officials detected and prevented that attempt. They tried to do it with Umar Faroukh Abdulmutallab, the underwear bomber, who went up in flames on Northwest Flight 253 on Christmas Day of 2009. Again, we were fortunate that his bomb did not detonate.

And these are just the plots that are publicly well-known. Many other efforts have been foiled at an early stage and have not become publicly known. The point is that al Qaeda and its affiliates are trying, and they will keep trying. Remember that al Qaeda tried to bring down the Twin Towers with a truck bomb in 1993 before they succeeded with airplanes on September 11. And all the criticism of TSA now – for being intrusive in trying to make sure that bombs don't get on airplanes – will be nothing like the criticism if the terrorists succeed in bringing down a plane.

The Response Is Proportionate

So what should be done in the face of this persistent threat? As each particular threat technique has emerged, we as a nation could have said "let's just keep doing what we're doing." But that would have been an invitation to disaster – we cannot stick our collective head in the sand. With clear evidence that terrorists will try to hide explosives in their shoes, it just makes sense to screen passengers' shoes. Removing shoes is annoying, but not overly burdensome in view of the threat. And we've been living reasonably well with this response for almost 10 years.

With each new threat technique, it is appropriate to consider a range of possible responses and to ensure that the chosen response is sensible in view of the magnitude of the threat, the technology available to counter it, and the burden and cost to the traveling public.

The response to the liquid explosives plot is another example of a reasonably calibrated response. When British and U.S. intelligence and law enforcement agencies determined that there was a plot to bomb airplanes using liquid explosives, the first order of business was to stop that plot. And they did that. But as good as these intelligence and law enforcement organizations are – and they are quite good – we cannot be certain that we will detect all plots in advance. So the next order of business was to determine what measures would be needed to thwart similar liquids plots in the future.

There were some who wanted to ban virtually all liquids on planes. That would have been one way of dealing with the threat. But it would have been quite onerous for the traveling public. And rigorous analysis of the threat led to the conclusion that reasonable security against liquid explosives could be ensured by prohibiting passengers from carrying on board liquid containers of more than three ounces.

Living with this rule is a pain, to be sure. It would be better if there were a reliable technology that could quickly detect liquid explosives and allow passengers to carry safe liquids on board. I know that TSA does not like collecting tubes of toothpaste. But no liquid explosives detection technology is yet ready for deployment. So air passengers likely will have to deal with the liquids rules for some time to come. That's unfortunate, but it would be far more costly to stick our collective head in the sand and hope that no one blows up a plane.

That leads me to TSA's use of Advanced Imaging Technology. We have known for some time that magnetometers – metal detectors – are important security devices but are not sufficient to detect some types of explosives that can be hidden in a passenger's clothing. Research and testing to develop better, safer, more effective passenger screening tools has been underway in earnest since 9/11, and TSA began deploying Advanced Imaging Technology in 2007. But it took the near-disaster of the Christmas Day underwear bomber to accelerate deployment. The explosives he used cannot be detected by a standard metal detector. Here again, the change in passenger screening –

through broad deployment and flexible use of advanced imaging technology – was calibrated to the threat.

Of course, TSA could have chosen other responses, but those other responses do not seem appealing. TSA could have, for example, done nothing at all to change passenger screening. The underwear bombing incident did not end in disaster, thanks to faulty ignition by the would-be bomber and fast action on the part of heroic passengers. TSA could have chosen to wager on al Qaeda's continued incompetence. But it would be wagering with passengers' lives, and that is not a bet the public wants TSA to make.

At the other end of the range of possible responses, TSA could have insisted that every person be subject to scanning with the new technology before boarding a plane, or TSA could have insisted that every passenger be subject to a very intrusive physical search. But these types of mandates would have caused an even greater uproar from the traveling public.

Instead, TSA chose a reasonable course – broad deployment of the new technology with randomized and flexible use. Not every passenger is selected for scanning – generally TSA uses randomization procedures to create a sufficient likelihood of detection such that the deterrent effect is high. And for those passengers that are selected, there is flexibility: the passenger can choose a thorough pat-down instead of the scan.

I have been through both the scanners and the TSA enhanced pat-down process. The patdown was highly professional and, to my mind, not especially intrusive. I prefer to be scanned, though, and I'd recommend that process to anyone concerned about the patdown. TSA deserves credit for offering passengers that choice.

TSA also deserves credit for the scope of privacy protections it has implemented. The TSA officers who see the passengers do not see the scans of the passengers; rather, the results of each scan are relayed to the screener by a TSA officer who is located remotely. And the scanning technology blurs or removes facial features of the passengers, so that even the remotely located officers cannot identify the passengers by face. Further, TSA policies prevent storing or transmitting the images of passengers. Finally, future generations of the scanning technology will simply identify anomalies without the outlines of the passenger's body – those outlines likely will be replaced with cartoon figures or stick figures.

The "Privacy" Concern Is Counterproductive

In short, critics are making a privacy mountain out of a molehill – a molehill that is likely to shrink even smaller once the next generation of Advanced Imaging Technology comes online.

The more pointed criticism comes from those who say that better scanning technology is not a complete solution. It is possible to find weapons and hiding places that even the

scans and the patdowns won't discover. We should not spend all our time looking for weapons. We need to spend more time looking for terrorists.

This is not a new idea. In 2003, for example, the Bush administration announced a second generation of the Computer Assisted Passenger Prescreening System, or CAPPS II. CAPPS II would have analyzed passengers' travel histories and travel plans to identify possible terror suspects and screen them with particular care. By focusing on suspected terrorists, CAPPS II could have mitigated the burdens imposed on ordinary travelers.

But the CAPPS II program was stopped dead in its tracks by privacy groups – those on the far left and far right – who claimed that TSA could not be trusted with data about who was checking in, where they had traveled, and where they planned to go. Today, as a result of this concerted campaign, TSA does not have access to sufficient passenger information to identify risky travelers. And so it has been forced to treat all of us as though we are all potential terrorists.

I want to stop for a moment to point out the irony. Some of the same groups and people who campaigned against letting TSA use travel data to distinguish among passengers are here today criticizing TSA for treating everyone with an equal degree of suspicion.

It is worth asking again why the use of ordinary data, such as travel histories and plans, is so controversial. As many have observed, treating all travelers as equal threats to aviation security is neither effective nor efficient. TSA's sister agency – the US Customs and Border Protection (CBP) – has been using passenger data for years to decide how much scrutiny to give passengers who are traveling to the United States from a foreign country. CBP has used that information to help thwart many recent terrorist attempts. What is so different about TSA that it can't be trusted with similar information – especially if using the information would reduce the need for other, more immediate intrusions?

I'm sure there are a few people who think it's worse for TSA to have their travel data than for TSA to pat them down or scan their bodies. I certainly don't, and I think the vast majority who feel the same way should have the option of providing that information if it will speed them through the airport. For that reason, as a further step in risk-based screening, TSA should consider implementation of a program that would enable travelers to voluntarily give TSA access to information about themselves in exchange for the possibility of quicker, less intrusive physical inspections.

I say the possibility of less intrusive inspections because we can never have a program that guarantees reduced levels of inspection. That would make the program too attractive for would-be terrorists. We will always need some random checks to discourage al Qaeda from trying to game the system. But travelers who have provided additional information are likely to be less risky, and so they could be subjected to streamlined screening most of the time. This is really not different from the use of scanners on a

random rather than universal basis. For trusted travelers who have provided access to their data, the chances of a detailed screen would be greatly reduced.

I don't want to try to design such a system in detail, but let me sketch one possibility for the committee. Imagine you are among the majority who don't see what the fuss over travel data is about. You authorize TSA to access data about you –travel data, say, and perhaps criminal or other records. When you show up for your flight, your boarding pass has already been coded to show that you're entitled to use the trusted traveler lane.

Good thing, too, because that line is much shorter. The TSA official checks your ID and boarding pass as usual, but he waves you into a fast lane, where the most aggravating and time-consuming security procedures have been eliminated – the liquids and laptop inspections, perhaps the shoe inspection too. No wonder the trusted traveler line is shorter; it is moving twice as fast. Every once in a while, though, scanning the boarding pass sets off a beep, and the officer waves you into a standard line for the usual drill. This is a random event, programmed into the system in advance based on all the data that TSA has. The line is still a lot faster, because only a few of the trusted travelers end up in the standard inspection, but that random event makes it difficult for terrorists to game the trusted traveler program.

The upshot would be faster inspections, less hassle, and more security. More privacy too, for those who think that giving up a little information is a fair trade for fewer scans and patdowns.

I support TSA's use of Advanced Imaging Technology and, more broadly, its well-calibrated responses to each new threat technique. But in the end, more intelligent TSA screening, using traveler data, gives us the best chance to thwart the next attack.

STEWART A. BAKER

Stewart Baker is a partner in the law firm of Steptoe & Johnson. He is the author of *Skating on Stilts – Why We Aren't Stopping Tomorrow's Terrorism*, a book on the security challenges posed by technology and the use of data in preventing terrorism.

From 2005 to 2009, he was the first Assistant Secretary for Policy at the Department of Homeland Security. As assistant secretary, Mr. Baker oversaw offices responsible for Department-wide policy analysis, international affairs, strategic planning, and relationships with private sector, advisory committees, and law enforcement. He was heavily involved in all aspects of the Department's activities, including aviation security.

Mr. Baker's practice covers national and homeland security, electronic surveillance, law enforcement, export control, encryption, and related technology issues. He advises clients on US export controls, on the Communications Assistance for Law Enforcement Act ("CALEA"), and on the requirements imposed by CFIUS, among other issues.

During 2004 and 2005, Mr. Baker served as General Counsel of the WMD Commission investigating intelligence failures prior to the Iraq war.

From 1992 to 1994, Mr. Baker was General Counsel of the National Security Agency, where he led NSA and interagency efforts to reform commercial encryption and computer security law and policy.

Mr. Baker has testified before government agencies and committees on many occasions, including the 9/11 commission on intelligence and has served on numerous boards and commissions, including the President's Export Council Subcommittee on Export Administration, the Industry Trade Advisory Committee on telecommunications and electronic commerce, two Defense Science Board panels on information warfare defense, and the Markle Task Force on Technology and Terrorism. He has also been an advisor to international organizations such as the International Telecommunications Union, and the Organisation for Economic Co-operation and Development. He has served as a Distinguished Visiting Fellow at the Center for Strategic and International Studies and as a Visiting Fellow at the Hoover Institution.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name:

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2008. Include the source and amount of each grant or contract.

None

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

None

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2008, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

None

I certify that the above information is true and correct.

Signature:

Date: 15 March 2011