United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense, and Foreign Operations

Hearing on

TSA OVERSIGHT PART I: WHOLE BODY IMAGING

Washington, DC
March 16, 2011

Statement of Fred H. Cate
Distinguished Professor, C. Ben Dutton Professor of Law, and
Director, Center for Applied Cybersecurity Research, Indiana University;
Senior Policy Advisor, Centre for Information Policy Leadership at Hunton & Williams LLP

Chairman Chaffetz, Representative Tierney, and Members of the Subcommittee,

My name is Fred Cate, and I am a Distinguished Professor and C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law, and the director of Indiana University's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Education and in Information Assurance Research.

For the past 21 years I have had the privilege of researching and teaching about a variety of privacy, security, and other information law and policy issues. I served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, and counsel to the Department of Defense Technology and Privacy Advisory Committee.

In addition to my academic appointment, I am also a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, a member of Intel's Privacy and Security External Advisory Board, a member of the Department of Defense DARPA Privacy Oversight Board, a member of the Department of Homeland Security Data Privacy and Integrity Committee's Classified Cyber Review Subcommittee, editor of the Privacy Department of the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy*, and one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*, among other activities.

I am testifying today on my own behalf; the views I express should not be attributed to any organization with which I am affiliated.

Chairman Chaffetz, I want to begin by thanking for your leadership in holding this important series of hearings on the TSA, and for inviting me to participate in today's hearing on the TSA's use of whole body imaging technologies. The TSA is charged with helping to secure one of our nation's most essential infrastructures—air transportation—and the agency's activities touch more Americans, as well as most visitors to this country, in ways far more direct and intrusive than any other federal agency. The

TSA is unusual in its ability to search the persons and possession of individuals who have done nothing to warrant suspicion. Moreover, although it carries out much of its responsibility in public view, most TSA policies and processes are secret. In the face of the courts' traditional deference where security claims are involved and the administration's failure to nominate a full slate of members of the Privacy and Civil Liberties Oversight Board, oversight by Congress is not merely important, it is in fact the only independent guaranty that taxpayers and the traveling public have that the TSA is conducting its activities effectively, legally, and appropriately.

I have been asked to address the effectiveness of whole body imaging through the use of advanced imaging technologies (AIT).

AIT Effectiveness

AITs use high-energy X-rays (or, in some cases, other types of energy) designed to penetrate a traveler's clothing, but not his or her body (or not too far into his or her body—unlike medical X-rays). The goal is to reveal what the traveler has on his or her person.

When installed, calibrated, used, and maintained properly, AITS may be effective at achieving this goal. We don't know, because the TSA will not make public its evaluative studies and the equipment manufacturers do not make machines available for independent testing. Moreover, proper installation, calibration, use, and maintenance are important qualifications that should not be taken lightly.

Even if AITs live up to their technological potential, it is important to be clear about how limited that potential is. For example, AITs do not detect explosives. They do not detect firearms. They do not distinguish dangerous from ordinary materials. All they are technologically capable of doing is calling attention to "anomalies" on the person of the traveler.

As a result, the real answer to the question of effectiveness turns on what the TSA does with the information provided by AITs—how AITs are integrated into a broader system of air transport security. We know more about this, and most of what we know suggests that AITs are generally not effective at contributing to greater security of airplanes and airports. In fact, it appears that the way in which the TSA has deployed these machines actually may be undermining the security of the U.S. air transportation infrastructure.

Too many false positives

There are many reasons why this is true, most of which relate to the fact that because the machines consider an "anomaly" as anything on a person, they generate numerous false positives. A piece of tissue, a dollar bill, a folded pocket, a boarding pass, a piece of candy—all are "anomalies" in the world of AITs, as deployed by the TSA, and so have to "cleared." Ironically, the old-fashioned metal detectors that the TSA is retiring are not fooled by such "anomalies."

The numerous false positives in turn divert TSA agent attention away from potential real threats towards "anomalies" that clearly pose no threat whatever. The goal in security is always to focus scarce resources on the greatest risks, but the TSA's deployment of AITs has precisely the opposite effect: it tends to focus TSA agent attention on innocuous "anomalies."

Moreover, in an effort to avoid so many "anomalies," the TSA now has passengers removing more and more clothing and other possessions before going through the scanners. Even though AITs were sold to the American public with the promise that they can see through clothing, passengers must remove outer garments because different thicknesses of clothing generate even more "anomalies." Belts are another offender that must now go, even if they do not have a large metal buckle. TSA agents are having to spend more time undressing passengers so that the new 21st-century detection technology won't generate quite as many erroneous alerts. This requires more agents and more money, in addition to the cost of the machines, and it diverts agents and resources from more appropriate and effective security tasks.

An inability to clear "anomalies"

But even if there were only a few "anomalies" detected by AITs, it turns out that the TSA has little ability to actually "clear" many of them. I was reminded of this just last week at Reagan Washington National Airport when the AIT discovered a loose aspirin in my shirt pocket. This anomaly called for a pat down. The agent felt the pill and said "what is this?" I said "aspirin" and he politely waived me through. It could just as easily have been potassium cyanide: neither the AIT nor the TSA agent has any process or equipment for determining the difference.

We have spent more than $2 billion installing a technology to identify "anomalies" that we cannot practically evaluate for the risk they pose. It was this inability to clear many of the false positives identified by AITs that led to the TSA's disastrous policy begun last October of intimate, intrusive searches. The problem is that despite their intimacy, the searches did nothing to help the agent determine whether the "anomaly" was a real risk or just another false positive.

This is especially clear in the case of people with medical devices or prosthetics. As a diabetic on an insulin pump—a device the size of a pager strapped to my waist that provides life-sustaining insulin—under the TSA's October policy, an agent would search me head to toe, including a careful pat-down of my genitals—as if somehow my genitals have become suspicious because I use an insulin pump. At the end of the search, however, the agent has no better idea than he did at the beginning whether the pump is loaded with insulin or high-tech explosives.

After two months of this policy, the TSA shifted ground and determined that insulin pumps would not require a full body search, but instead would be swabbed and the swab tested for explosive residue. A colleague of mine who works for the federal government and is also a diabetic described the indignity of recently having a TSA agent at Dulles International Airport reach inside her underwear with the swab. To what end? Are insulin pump users more likely than other travelers to secret explosives on their bodies? And what happened to the much-vaunted AIT machines that were supposed to detect the presence of such explosives? Why are we now swabbing inside travelers' underwear as well as using AITs to peer inside, especially when there is no sign of any "anomaly" from either technique?

I have found it easier and far less intrusive to simply remove my insulin pump before being required to undergo AIT screening. (I don't remove it before passing through a metal detector because it doesn't trigger any alarm.) I am fortunate to have this option; most travelers with medical devices or prosthetics aren't so lucky. But I am still left with the tiny plastic cannula in my abdomen to which the pump connects. The AIT sometimes—interestingly, not consistently—identifies this as an "anomaly." When it does, a TSA agent pats me down, feels the sensor, and says "what is this?" I say "an insulin cannula" and the agent invariably politely waives me through. The agent has no idea, no verification,

and no certainty what is actually taped to my stomach. I am "cleared" not because the agent has determined that the plastic tube poses no danger, but because there is no way a TSA agent can make any further determination.

Many travelers suffer far greater indignities due to physical searches, triggered by AIT "anomaly" detection, that reveal nothing about whether the "anomaly" poses a threat. For example, after agents finish inspecting the breasts of a woman with an implant, they have not better idea whether the implant is filled with liquid explosives or silicone. The same is true with prosthetic limbs, urostomy bags, and most other medical appliances.

This type of response to having the AIT identify something as an "anomaly" is the very definition of "security theater"—it looks like the agency is doing something, but it accomplishes nothing. The same is true with many, perhaps most, of the searches that are triggered by AIT "anomalies." A rational person might question whether it is worth the money we are spending to identify "anomalies" if the vast majority of them (indeed, perhaps all of them) are false positives, and we lack the practical ability to follow up on many of them in any event. This is the height of ineffectiveness.

The technological limits of AITs

One of the fundamental questions that security experts ask about detection technologies is how easily they can be evaded. The answer with AITs appears to be "pretty easily." Because their radiation is supposed to stop at the skin, AITs are useless for locating explosives hidden in body cavities. Researchers in Europe have shown that this includes the mouth, and were able to pass solids and liquids through security undetected merely by holding them in their closed mouths. As security authority Bruce Schneier, originator of the phrase "security theater," has written in the *Atlantic*: "A terrorist can go through the scanners a dozen times with bits in his mouth each time, and assemble a bigger bomb on the other side. Or he can roll it thin enough to be part of a garment, and sneak it through that way. These tricks aren't new."[1]

Similarly, liquid explosives are not addressed by AITs. The TSA currently has no way of determining what is in the liquids passengers put through X-ray machines or buy once they have passed through security, and are left to hoping that terrorists will not think to combine the contents of their one-quart bags once they are onboard an aircraft or of infiltrating the large drink bottles that are sold beyond security in airports.

So while AITs have been deployed in the United States to deal with the 2009 attempted underwear bomber—and there is wide-ranging disagreement about whether the technologies or the subsequent searches would in fact have detected the thin plastic explosive sheets that case involved—the TSA is counting on terrorists not developing any new strategies. We are literally spending billions fighting yesterday's threats on the assumption that terrorists are neither smart nor innovative.

[1] Bruce Schneier, "Why the TSA Can't Back Down," *Atlantic*, Dec. 2, 2010, available at http://www.theatlantic.com/national/archive/2010/12/why-the-tsa-cant-back-down/67337/

And we don't seem to be succeeding at even that backwards-looking task. According to information leaked by the TSA in February 2011, an undercover TSA agent was able to carry a firearm secreted in her underwear through AIT screening at the Dallas-Fort Worth Airport every time she tried.[2]

Poor policies undermine good security

The TSA leadership has insisted that its AITs generate real body images that look akin to X-rays and include the identifiable features of the passenger. Despite privacy concerns, the agency argued that only by having the complete picture could the agent make a determination as to whether "anomalies" were presented. This turns out not merely to be wrong, but to be counterproductive. The display of whole body and facial images has required blurring certain parts of the AIT image, thus limiting their effectiveness in revealing potentially suspicious "anomalies." Anecdotal reports suggest that actual facial and body characteristics may also distract TSA agents. European aviation security officials have managed to avoid these problems by deploying AITs that generate gingerbread person-like outlines without recognizable features, and then highlight with arrows or pulsing red indicators "anomalies" of the body of the traveler. These depictions may turn out to be more effective in alerting agents to potentially suspicious areas, and the TSA, despite its prior insistence on real whole body images, is now testing the new approach.

The TSA's determination to deploy AITs, whether or not they are effective, is not a new phenomenon. The AIT approach is only the most recent example of a series of intrusions that the TSA claimed were "necessary" to protect security, only to quietly recant them when it was shown that they did not work. Recall passenger profiling, bans on nail clippers and eyelash curlers, and expensive air puffers to detect explosive residue—all of which have now been abandoned.

Looking Ahead

While I am deeply critical of the TSA leadership and their use of AITs, I have great regard for many of the TSA agents I encounter. They are as disheartened as the public is about the poor policies being pursued by the TSA leadership. As one TSA agent in Indianapolis put it to me last November: "you wouldn't believe what we have to put up with from Washington. If those bureaucrats would spend even 15 minutes in the field, they would quickly realize how silly many of their policies are."

I also don't want my criticism of the TSA's poor choices to in any way obscure how important and difficult the agency's mission is. And to that end, I would like to offer two specific recommendations for the committee's consideration as you exercise your vital oversight responsibilities.

A clear mission

First, the TSA and ultimately the administration and Congress need to be clearer about what precisely that mission is. If it is to prevent the weaponization of passenger aircraft that occurred so tragically on September 11, 2001, many security experts believe that goal has been reached. Cockpit doors have been secured and passengers have been alerted to the danger and to their role in acting to

[2] Grant Stinchfield, "TSA Source: Armed Agent Slips Past DFW Body Scanner," NBC-DFW, Feb. 21, 2011, available at http://www.nbcdfw.com/news/local/TSA-Agent-Slips-Through-DFW-Body-Scanner-With-a-Gun-116497568.html.

protect their own security. That mission has been accomplished, and the TSA should not be selling AITs or any other technology on the basis that it is necessary to prevent the horrors of 9/11 from recurring.

If the TSA is now targeting the hijacking or destruction of an airplane, we should remember that the United States and many other nations have waged that battle for more than 30 years with great success without any help from AITs and without the intrusive physical searches that TSA implementation of AITs has led to. Moreover, it must be remembered that when so-called "shoe-bombers" and "underwear" bombers attempted to bring down planes, they failed. After-the-fact deployment of expensive technologies and burdensome procedures designed to thwart them is striking given that the attacks were unsuccessful in the first place, and would likely not have been prevented by these initiatives in any event since neither scanning shoes with X-ray machines nor people with AITs have been shown to detect either threat.

Perhaps more importantly, planes are already so full of potential weapons that it is irrational for the TSA to think they will ever make planes weapon-free, no matter how intimately the agency searches passengers. A sharpened pencil, the steel axle that runs through roll-aboard luggage wheels and laptop hinges, matches in the vicinity of aerosol sprays or oxygen tanks, a bomb in checked baggage—all pose a real threat. And real dangers, such as shoulder-fired missiles, exist outside of the plane as well. There is little the TSA is doing or could do against these dangers, but even the ones it can—like screening all checked baggage and freight on passenger planes, and conducting serious background checks of airport employees—seem to interest the agency less than more visible passenger searchers.

The TSA needs a clear, rational mission, and direct, serious oversight to ensure that it is focused on achieving that mission in a sensible, effective way. Massive expenditures targeting ineffective tools at yesterday's terrorist threats do little to advance security, they ignore far more real dangers that air travel involves and that could benefit from the scarce resources currently being focused on screening passengers, and they undermine public confidence and public trust.

Clear processes for determining effectiveness

One good way to achieve this goal, and my second recommendation to this committee, would be for Congress to require the TSA to follow basic requirements for evaluating the effectiveness of not only AITS but all of its initiatives. The National Academy of Sciences addressed the issue of security programs that relied on personal data or searches in a report published in 2008 and its first recommendation was that "U.S. government agencies should be required to follow a systematic process . . . to evaluate the effectiveness, lawfulness, and consistency with U.S. values of every information-based program, whether classified or unclassified, for detecting and countering terrorists before it can be deployed, and periodically thereafter." [3]

As a member of that committee, I could not agree more strongly with that recommendation. In fact, the NAS committee went so far as to propose a framework for evaluating effectiveness and privacy impact of new systems and technologies. Ironically, given that the Department of Homeland Security was the primary funder of the study, the recommendations and the proposed framework have been ignored by DHS and by Congress. I urge you to revisit that proposed framework—crafted by a bipartisan

[3] Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Academy of Sciences, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (2008).

panel of experts in terrorism, security, data analysis, intelligence, privacy, law, and law enforcement from public and private sectors—and consider whether it might serve as a basis for improving the quality of both the TSA's operations and this committee's oversight.

Here is the outline of the effectiveness portion of the framework from the NAS report, which would apply to all "informed-based programs," including AITs:

1. Is there a clearly stated purpose for the information-based program?
   - Is that objective meaningful?
   - Is it appropriate?
   - Is there demand or need for it?
   - Is it already being accomplished or could it be accomplished through less intrusive or costly means?

2. Is there a sound rational basis for the information-based program and each of its components?
   - Is there a scientific foundation for the system?

3. Is there a sound experimental basis for the information-based program and each of its components?
   - Does the system work to achieve its stated purpose?
   - Has a new system been shown to work simulations or laboratory settings or has it been field-tested?
   - Did the test conditions take into account real-world conditions?
   - Has it been applied to historical data to determine if it accurately accomplished its objective?
   - Have experimental successes been replicated to demonstrate that they were not coincidence?
   - Has the system been subjected to critical analysis, challenge, and likely countermeasures (for example, through "red-teaming")?

4. Is the information-based program scalable?
   - Has it been tested on a data set of adequate size to predict its scalability?
   - Has it been tested against likely countermeasures or changes in technologies, threats, and society?

5. Is there a clearly stated set of operational or business processes that comprehensively specify how the information-based program should operate within the organization?

6. Is the information-based program capable of being integrated in practice with related systems and tools?
   - Does the system interact effectively with the sources of information on which it relies?
   - If it requires combining data, can it do so in practice to yield meaningful results and at the speed necessary?
   - Can the end product of the system be acted upon meaningfully by people or other systems?

7. Is the information-based program robust?
   - Can it easily be compromised by user errors?

- Can it easily be circumvented by countermeasures?

8. Are there appropriate guarantees that the data on which the information-based program depends are appropriate and reliable?
   - Are there adequate guarantees of the information's validity, provenance, availability, and integrity?
   - Are the data easily compromised or manipulated so that the system can be defeated?

9. Does the information-based program provide for appropriate data stewardship?
   - Are the data protected from unlawful or unauthorized disclosure, manipulation, or destruction?
   - Are there technologies and/or procedures built into the system to ensure that privacy, security, and other data stewardship policies are followed?

10. Are there adequate guarantees of objectivity in the testing and assessment of the information-based program?
    - Has there been peer review or its equivalent?
    - Has the program been evaluated by entities with no stake in its success?
    - Have test results been evaluated by independent experts?
    - Was testing blind—to both researchers and research subjects—whenever possible?

11. Is there ongoing assessment of the information-based program?
    - Are there mechanisms for detecting and reporting errors?
    - Are there monitoring tools and regular audits to assess system and operator performance?

12. Have the effectiveness of the information-based program and its compliance with these key requirements been documented?
    - Has the documentation been examined by an entity capable of evaluating the scientific evidence of effectiveness outside of the agency promoting the new system.

The TSA appears to have avoided most of these straightforward steps. Moreover, the agency's claims that it has done testing in related areas—such as the health impact of AITs—have been undermined by denials or contradictory reports from the third parties that the TSA claimed to have engaged.[4] In short, the simple evaluative steps recommended by the NAS, which are widely followed today in both public- and private-sectors, could have avoided many of the missteps identified above, and might have highlighted for the agency, and for Congress, the shortcomings of the massive investment we have all been asked to make in AITs.

Conclusion

The experience with AITs to date is not comforting, not because the technologies are incapable of detecting "anomalies," but because they detect so many "anomalies"—almost everything about the traveling public is anomalous—and the TSA leadership has not yet figured out how to respond rationally to the deluge of false positives. It appears to have deployed AITs either before they were ready for use

[4] Andrew Schneider, "AOL Investigation: No Proof TSA Scanners Are Safe," *AOL News*, Dec. 20, 2010, available at http://www.aolnews.com/2010/12/20/aol-investigation-no-proof-tsa-scanners-are-safe/.

in the field or before the agency knew how to use them effectively. As a result, AITs are not merely failing in practice to protect the air transport infrastructure against threats, but are actually interfering with TSA agents' ability to do so by sending them on so many wild goose chases and diverting their attention from more likely threats. In short, too many agents are working to satisfy the demands of AITs, rather than AITs being used to facilitate the important work of TSA agents.

The problem is bigger than just the TSA's deployment of AITs. Because the agency appears to lack a clear, coherent, rational mission, or a laser-like focus on achieving that mission, AITs are only the most recent example of big-ticket distractions that the agency has introduced to the travelling and tax-paying public. A more focused mission and greater congressional oversight of the TSA are critical to ensure that air transportation is appropriately secured against likely attacks and public resources spent wisely.

To be sure, the TSA has a vital and difficult task, but it has extraordinary resources and powers to carry out that task. The framework published in 2008 by the NAS is one tool that both the TSA and Congress should consider for helping to ensure that the agency uses its significant resources wisely and effectively, especially where the health and privacy, as well as security, of the public are involved.

Thank you again for the opportunity to participate today.

Biography

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, Adjunct Professor of Informatics and Computing, and director of the Center for Applied Cybersecurity Research at Indiana University. He works at the forefront of privacy, security, and other information law and policy issues.

He is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, a member of Microsoft's Trustworthy Computing Academic Advisory Board, Intel's Privacy and Security External Advisory Board, the Department of Defense DARPA Privacy Oversight Board, the Department of Homeland Security Data Privacy and Integrity Committee's Classified Cyber Review Subcommittee, the Board of Directors of The Privacy Projects, and BNA's *Privacy & Security Law Report* Advisory Board. He serves as the Privacy Editor for the IEEE's (Institute of Electrical and Electronic Engineers) *Security & Privacy* and is one of the founding editors of the Oxford University Press journal, *International Data Privacy Law*. He holds a TS-SCI clearance.

Previously, Professor Cate served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention, reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information, counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities.

Professor Cate has testified before numerous congressional committees, and he speaks frequently before professional, industry, and government groups. He has spoken throughout the United States and in Belgium, Canada, China, Finland, France, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom. He is the author of more than 100 articles and books, including *Privacy in the Information Age, The Internet and the First Amendment*, and *Privacy in Perspective*. He appears regularly in national media.

Professor Cate is the President and a Fellow of the Phi Beta Kappa Society and an elected member of the American Law Institute. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is listed in *Who's Who in the World*, *Who's Who in America, Who's Who in American Law*, and *Who's Who in American Education*. *Computerworld* included him in its three most recent rankings of "Best Privacy Advisers."