U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation Security Administration

MAY 28 2010

Electronic Privacy Information Center, *et al.*
c/o Mr. Mark Rotenberg
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009

Dear Mr. Rotenberg:

Thank you for the letter of April 21, 2010, to Department of Homeland Security (DHS) Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan from 30 organizations regarding the Transportation Security Administration's (TSA's) use of advanced imaging technology (AIT) to screen passengers for security purposes at our Nation's airports.[1] I am responding on behalf of Secretary Napolitano and Chief Privacy Officer Callahan, and request that you forward this letter to the other organizations who signed the April 21 letter. We appreciate the opportunity to address the important issues the 30 organizations have raised regarding AIT.

Statutory Mandate. In your letter, you question TSA's authority to install and operate AIT machines for passenger screening at airports absent the initiation of a formal public rulemaking process under the Administrative Procedure Act (APA). However, TSA is not required to initiate APA rulemaking procedures each time the agency develops and implements improved passenger screening procedures. Current regulations require passengers and others to comply with TSA's procedures before entering airport sterile areas and other secured portions of airports.[2]

Moreover, since 9/11, Congress has mandated that TSA invest in technologies to strengthen the efficiency and security of aviation. The emphasis on developing new technologies to address transportation security is codified at 49 U.S.C. § 44925(a):

> The Secretary of Homeland Security shall give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property. The Secretary shall ensure that the equipment alone, or as part of an integrated system, can detect under realistic operating

[1] While you footnote that your letter is a Petition for Rulemaking under 5 U.S.C. §553, the relief actually sought is specified instead to be the immediate suspension of the AIT program. Accordingly, TSA does not interpret your letter to seek a rulemaking or to constitute a petition under 5 U.S.C. §553.

[2] *See* 49 CFR 1540.105(a)(2) and 1540.107.

> conditions the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.

The Secretary also is required under 49 U.S.C. § 44925(b) to develop a strategic plan for deploying explosive detection equipment, such as AIT machines, at airport screening checkpoints.

AIT equipment addresses this Congressional and national security mandate by safely screening airline passengers for both metallic and nonmetallic threats, including weapons, explosives and other objects concealed under layers of clothing. TSA, DHS, the White House, and the Congress are pursuing AIT for airport checkpoint security because it is a key component of TSA's layered approach to security that addresses the evolving threats faced by airline travelers. As Secretary Napolitano stated in January 2010:

> In and of itself, no one technology, no one process, no one intel agency is the silver bullet here. It's layer, layer, layer, layer. . . . [AIT is] good technology with behavior detection officers, with canines, with explosives detection equipment, with the right watch lists, with the right names on it and the right intel behind it. . . . [A]ll of these things have a role to play.[3]

Beyond the general mandate from Congress to deploy technology capable of screening airline passengers for nonmetallic and other evolving threats, DHS has communicated to and discussed with the Congress TSA's specific AIT deployment plans. For example, Secretary Napolitano recently announced deployments of AIT units purchased with American Recovery and Reinvestment Act (ARRA) funds to 28 additional airports, which will increase to 44 the number of airports with AIT equipment.[4] In addition, over the past several months, Secretary Napolitano and TSA Acting Administrator Gale Rossides have testified at Congressional hearings about AIT deployment plans and requests for funding for additional AIT deployment.

- "The . . . Recovery Act funds provided to TSA for checkpoint . . . screening technology have enabled TSA to greatly . . . accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security

---

[3] Hearing on "The State of Aviation Security - Is Our Current System Capable of Meeting the Threat?," before the Senate Committee on Commerce, Science, and Transportation, January 20, 2010.

[4] *See* "Secretary Napolitano Announces Additional Deployments of Recovery Act-Funded Advanced Imaging Technology," May 14, 2010, at www.dhs.gov/ynews/releases/pr_1273850925050.shtm. *See also* Secretary Napolitano's March 5, 2010 announcement of 11 airports that will receive AIT units using ARRA funds at www.dhs.gov/ynews/releases/pr_1267803703134.shtm.

authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010."[5]

- The President's FY 2011 funding request will result in "total AIT coverage at 75 percent of Category X airports and 60 percent of the total lanes at Category X through II airports."[6]
- "TSA is aggressively pursuing the deployment of enhanced screening technology to domestic airports and encouraging our international partners to do the same. While no technology is guaranteed to stop a terrorist attack, a number of technologies, when employed as part of a multi-layered security strategy, can increase our ability to detect dangerous materials. To this end, TSA is accelerating deployment of AIT units to increase capabilities to identify materials such as those used in the attempted Dec. 25, 2009 attack. These efforts are already well underway. . . . The President's FY 2011 budget requests . . . an additional 500 AIT units at checkpoints, . . . [and a]n additional . . . 5,355 TSO positions to operate these AIT machines at their accelerated deployment pace."[7]

As this discussion illustrates, TSA not only has ample, clear authority to install and operate AIT machines for passenger screening at airports, but has been directed by the Congress to pursue screening technology solutions that are capable of detecting nonmetallic and other dangerous devices under realistic operating conditions. DHS and TSA have communicated regularly with the Congress on TSA's AIT deployment efforts and recommendations. AIT machines offer the best current option for meeting these statutory directives and security imperatives.

AIT Screening is Optional. Your letter also states that AIT screening subjects all air travelers to intrusive searches that are disproportionate and for which TSA lacks any suspicion of wrongdoing. Your letter, however, misstates the facts.

TSA has made clear from its earliest AIT deployment that **use of AIT screening is optional for all passengers**,[8] and TSA makes every effort to address any AIT complaints or concerns.

---

[5] Written statement of Secretary Janet Napolitano for a hearing entitled "The State of Aviation Security - Is Our Current System Capable of Meeting the Threat?," before the Senate Committee on Commerce, Science, and Transportation, January 20, 2010.

[6] Written statement of Secretary Napolitano for a hearing on the DHS Budget Submission for FY 2011, before the Senate Committee on Homeland Security and Governmental Affairs, February 24, 2010, and before the House Homeland Security Committee, February 25, 2010.

[7] Written statement of TSA Acting Administrator Gale Rossides for a hearing on the TSA FY 2011 Budget before the House Appropriations Subcommittee on Homeland Security, March 4, 2010. *See also* Department of Homeland Security, Transportation Security Administration, Fiscal Year 2011 Congressional Justification for Aviation Security, pages AS-4, AS-13, and AS-22, and the written statement of Acting Administrator Rossides for a hearing entitled "The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening," before the Senate Committee on Homeland Security and Governmental Affairs, Wednesday, March 10, 2010.

[8] *See* www.tsa.gov/approach/tech/imaging_technology.shtm.

For those passengers who express concerns or decline AIT screening, TSA employs alternative screening techniques, such as use of a hand-held metal detector coupled with a pat down. The notion of alternative screening methods is consistent with TSA's screening practices over the years and is not a new feature that was introduced with the implementation of AIT. For example, TSA offers the pat down option to passengers who elect not to undergo screening by a walk-through metal detector (WTMD), and offers screening guidance for airline passengers with certain medical devices who may not wish to be screened by WTMD.[9] Not surprisingly, passengers with implanted knee and hip joints have welcomed AIT screening; these passengers alarm a WTMD and require a pat-down to resolve the alarm, but are able to use the AIT without alarming it.[10]

Similarly, options for alternative screening also are offered to those passengers for whom there are religious or cultural considerations. These passengers also may request an alternative personal search (pat-down inspection) performed by an officer of the same gender, and in private.[11]

In addition to being optional, AIT screening is widely accepted by the traveling public. For example, a *USA Today*/Gallup poll found that 78 percent of U.S. air travelers approve of the use of AIT screening in U.S. airports as a measure to prevent terrorists from smuggling explosives or other dangerous objects onto airplanes.[12] This result is consistent with TSA's experience with passenger acceptance rates for AIT machines at airport checkpoints. Only a small fraction of the millions of passengers screened using AIT, approximately 600 individuals, have expressed complaints or concerns about AIT since the inception of the program. This small number equates to less than .015 percent of the millions of airline passengers screened with AIT.

Effectiveness of AIT Screening. In your letter, you also express concern about the effectiveness of AIT devices, including whether they are capable of exposing the emerging threats to aviation such as powdered explosives, and state that there are less intrusive and costly techniques to address the risk of concealed explosives on aircraft. TSA continually searches for effective technologies and methods to detect explosives to meet the constantly evolving threats to transportation security. Clearly, walk-through metal detectors are not effective in detecting the kind of powdered explosive that you identified, and TSA's experience is that AIT provides the best, current tool for detecting this and other non-metallic threats. TSA's web site includes

---

[9] *See* www.tsa.gov/travelers/airtravel/specialneeds/editorial_1374.shtm#1. For example, for passengers with pacemakers, TSA recommends that individuals ask the TSO to conduct a pat-down inspection rather than using the walk-through the metal detector. TSA also recommends that passengers advise the Transportation Security Officer (TSO) if they have implanted pacemakers or other medical devices and where that implant is located so that a private screening can be offered. *Id.*

[10] *See* www.tsa.gov/approach/tech/imaging_technology.shtm.

[11] See www.tsa.gov/travelers/airtravel/assistant/editorial_1037.shtm.

[12] *See* "In U.S., Air Travelers Take Body Scans in Stride," Jan. 11, 2010, found at www.gallup.com/poll/125018/Air-Travelers-Body-Scans-Stride.aspx.

examples of the kind of materials that have been uncovered using AIT machines at U.S. airports, including bags of powder.[13]

Your letter also references a letter from Senator Collins and others to Secretary Napolitano about the use of AIT with automated target recognition (ATR) capabilities. Some machines with this feature currently are in use at Schiphol International Airport in Amsterdam. As the Secretary's response states,[14] TSA has worked closely with Dutch authorities and AIT manufacturers to evaluate ATR capabilities, and has established ATR requirements and provided them to AIT manufacturers. TSA is evaluating the effectiveness of ATR with respect to improved threat detection capabilities; should our evaluation show that ATR is effective in high-volume U.S. airport environments, TSA will seek to deploy this technology on AIT machines at U.S. airports.

TSA's experience, and that of other governments, clearly supports the effectiveness of AIT machines in exposing emerging threats to aviation, and this capability may be enhanced in the future by ATR, which TSA has been evaluating for some time. Your letter offers no other suggestions for alternative devices or practices that are less intrusive and less costly, yet equally effective, in addressing the risks to aviation security.

AIT Screening and Health Concerns. Your letter cited concerns about health issues related to AIT use involving children and pregnant women. TSA has relied on independent studies to address health concerns related to this technology to ensure the technology conforms to national consensus standards. Current AIT machines deployed by TSA use two different technologies: backscatter x-ray machines use ionizing radiation, and millimeter-wave machines use radio frequency energy.

AIT backscatter scanners use a narrow, low-level x-ray beam that scans the surface of the body at a high speed. The machines then generate an image resembling a chalk etching with a privacy filter applied to the entire body. Unlike a traditional x-ray machine that relies on the transmission of x-ray through the object material, backscatter x-ray detects the radiation that reflects back from the object to form an image.

Over the past several years, various backscatter scanners have been independently evaluated by the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH), and by the National Institute for Standards and Technology (NIST) on behalf of TSA. The backscatter scanner deployed by TSA, the Rapiscan Secure 1000 Single Pose, was independently evaluated by the Johns Hopkins University Applied Physics Laboratory (APL). The APL results confirm that radiation doses to the general public are well below those limits specified by standards established by the American National Standards Institute and through the Health

---

[13] See http://blog.tsa.gov/2009/07/blog-post-archives.html. It is unclear how you conclude that AIT cannot detect explosives in powder form. The TSA acquisition documents you cite to specify that AIT detects explosives, including liquids, solids, and powders.

[14] *See* Secretary Napolitano's April 27, 2010 letter to Senator Collins, attached to this letter (identical letters were sent to Senators Kyl and Chambliss).

Physics Society (ANSI/HPS) and published in ANSI/HPS N43.17-2009, entitled "Radiation Safety for Personnel Security Screening Systems Using X-ray or Gamma Radiation." The dose limits were set with the understanding that the general public includes individuals who may be more susceptible to radiation-induced health effects, such as pregnant and potentially pregnant women, children, and persons receiving radiation treatment for medical conditions. The amount of radiation from the backscatter screening equipment currently deployed by TSA is less than ten microrem, or the amount of radiation dose one would receive in less than two minutes of flight time on an airplane at flight altitude, or during one hour standing on the earth with normal exposure to naturally-occurring background radiation at sea level.

Millimeter wave AIT scanners use radio frequency energy in the millimeter wave spectrum to generate a three-dimensional computer image of the body based on the energy reflected from the body. The energy projected by millimeter wave technology is thousands of times less than the energy projected from a cell phone transmission, and far below the standards set by the Institute of Electrical and Electronics Engineers (IEEE) and the International Commission on Non-Ionizing Radiation Protection (ICNIRP).[15] TSA requires that millimeter wave AIT equipment be tested by independent, third-party labs to assure that the equipment meets the IEEE and ICNIRP standards for safety.

In summary, AIT scanning has been assessed by independent scientific entities that have found the technology conforms to national consensus standards.

Constitutional and Legal Issues. The deployment of AIT machines responds to the Congressional and national security mandate to screen airline passengers for both metallic and nonmetallic threats. Despite widespread public acceptance of AIT screening, TSA also provides alternative screening methods. AIT screening has proven effective, and numerous independent studies have addressed health concerns related to AIT screening.

In addition to this objective, factual support for the use of AIT screening, TSA has carefully considered the important Constitutional and statutory concerns raised in your letter as it developed AIT deployment plans. We disagree with your assertions that TSA's deployment of AIT equipment violates the Constitution and various laws, as addressed below.

The Fourth Amendment. TSA strongly disagrees with the statements in your letter that TSA's deployment of AIT machines violates the Fourth Amendment and subjects air travelers to unreasonable searches. Case law supports TSA's analysis.

TSA screening protocols at airport checkpoints have been upheld by the courts as "special needs searches" or "administrative searches" under the Fourth Amendment. *See, e.g., United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007) (*en banc*); *United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2006) (Alito, J.); and *Torbet v. United Airlines*, 298 F.3d 1087 (9th Cir. 2002). A lawful special

[15] See Institute of Electrical and Electronics Engineers (IEEE), C95.1 – 2005, Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz, revision of C95.1-1991 (Active), and International Commission on Non-Ionizing Radiation Protection (ICNIRP), Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields (Up to 300 GHz). Health Physics 74 (4): 494-522, April 1998.

needs search requires no warrant and no suspicion of wrongdoing. As long as the search serves a special public need beyond law enforcement and is conducted in a reasonable fashion, it will be found to be permissible under the Fourth Amendment. As stated by the Supreme Court:

> Our precedents have settled that, in certain limited circumstances, the Government's need to discover such latent or hidden conditions, or to prevent their development, is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion. *NTEU v. Von Raab*, 489 U.S. 656, 668 (1989).

Although the Supreme Court has not had occasion to rule directly on airport security screening, it has referenced security screening favorably in several cases:

> The point is well illustrated also by the Federal Government's practice of requiring the search of all passengers seeking to board commercial airliners, as well as the search of their carry-on luggage, without any basis for suspecting any particular passenger of an untoward motive... When the Government's interest lies in deterring highly hazardous conduct, a low incidence of such conduct, far from impugning the validity of the scheme for implementing this interest, is more logically viewed as a hallmark of its success. *Von Raab*, 489 U.S. at 675, n.3.

> We reiterate, too, that where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as "reasonable" – for example, searches now routine at airports and at entrances to courts and other official buildings. *Chandler v. Miller*, 520 U.S. 305, 323 (1997).

The Federal appellate courts that have directly considered the lawfulness of airport security screening have had little difficulty concluding that screening is a special needs search that serves a compelling public interest:

> When the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, the danger alone meets the test of reasonableness, so long as the search is conducted in good faith for the purpose of preventing hijacking or like damage and with reasonable scope and the passenger has been given advance notice...so that he can avoid it by choosing not to travel by air. *U.S. v. Edwards*, 498 F.2d 496, 500 (2d Cir. 1974).

> First, there can be no doubt that preventing terrorist attacks on airplanes is of paramount importance. Second, airport checkpoints also "advance[] the public interest" ...As this Court has held, "absent a search, there is no effective means of detecting which airline passengers are reasonably likely to hijack an airplane." *U.S. v. Hartwell*, 436 F.3d at 179-80.

Because airport security screening serves the compelling public interest of aviation security, it is a valid special needs search and a particular screening method will be lawful as long as it is reasonable.

> A particular airport security screening search is constitutionally reasonable provided that it is "no more extensive or intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives [] [and] that it is confined in good faith to that purpose." (citation omitted)...The search procedures used in this case were neither more extensive nor more intensive than necessary to rule out the presence of weapons or explosives. *Aukai*, 497 F.3d at 962.

In assessing the lawfulness of a particular search, it is important to note that the standard is whether it is reasonable, not whether it is the "least restrictive means:"

> [T]he choice among such reasonable alternatives remains with the governmental officials who have the responsibility for limited public resources. ("[T]he effectiveness inquiry involves only the question of whether the [search] is a 'reasonable method of deterring the prohibited conduct;' the test does not require that the [search] be 'the most effective measure.'")...Thus, our task is to determine not whether LCT's ASP [the screening plan at issue] was optimally effective, but whether it was reasonably so. (citations omitted) *Cassidy v. Chertoff*, 471 F.3d 67, 85 (2d Cir. 2006) (Sotomayor, J.) (upholding screening of ferry passengers).

Turning to the use of AIT, it is clear from the case law that this screening process is a lawful special needs search that strikes the appropriate balance between the interests of aviation security and individual privacy. As made clear by the attempted attack on December 25, 2009, the threat of nonmetallic explosives is real. Also, the nonmetallic threat is not limited to explosives. It is essential for aviation security to have screening methods in use that are capable of detecting threats in the form of powders, liquids, and other nonmetallic materials. The need for AIT also is illustrated by the fact that Congress has mandated TSA to deploy screening methods that are capable of detecting explosives and other nonmetallic threats. See 49 U.S.C. § 44925(a), quoted above. When compared to the substantial risk presented by the threat of terrorist acts against aviation, the impact on individual privacy of AIT screening is minimal. AIT screening has been appropriately tailored to minimize the impact on individual privacy while still providing an effective means of detecting concealed nonmetallic threats. Given the nature of the threats we face today, AIT screening is "no more extensive or intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives." *Aukai*, 497 F.3d at 962.

The Privacy Act. Contrary to your assertions, TSA has not violated the Privacy Act in its AIT deployment. The Privacy Act applies to systems of records in which the records are retrieved by the name or personal identifier of the individual. 5 U.S.C. §552a(a)(5). All Privacy Act requirements, including publication of a system of records, are linked to the agency maintaining a system of records. AIT does not collect and retrieve information by a passenger's name or other identifying information assigned to that individual, nor do we link any AIT images to any personally identifying information about the individual, such as name or date of birth. Indeed, images are not retained and all images are immediately deleted after AIT screening is complete. Consequently, since TSA does not maintain a system of records by using AIT, none of the obligations outlined under section 552a(e), "Agency requirements," apply to TSA.

TSA and DHS, including the DHS Chief Privacy Officer, evaluated the privacy considerations associated with AIT very carefully before TSA deployed the technology. As a result, TSA incorporated robust privacy protections into the program. These protections are reflected in the publicly available Privacy Impact Assessment (PIA), which was published two years ago under the authority given to the Chief Privacy Officer to assess the impacts of technology on privacy, in advance of the deployment of AIT at airports.[16] The PIA outlines a number of measures that TSA has implemented to ensure passenger privacy, and reflects extensive consideration of informal comments from a wide variety of sources, including some of the groups that have signed your letter. Relevant operating protocols include:

- The TSO viewing the images is located remotely from the individual being screened to preserve anonymity and modesty.
- To resolve an anomaly, the TSO viewing the image communicates via radio to direct the TSO at the checkpoint to the location on the individual's body where a threat item is suspected.
- The images are immediately deleted once AIT screening of the individual is complete.
- The image storage functions are disabled by the manufacturer before the AIT equipment is placed in an airport. This function cannot be activated by the TSOs operating the equipment. Your claims regarding storage of images by AIT used in TSA test facilities are irrelevant to the operation of the devices in the airports. As stated in the AIT PIA, "While the equipment has the capability of collecting and storing an image, the image storage functions will be disabled by the manufacturer before the devices are placed in an airport and will not have the capability to be activated by operators."
- Images cannot be downloaded in operating mode, and the equipment is not networked.
- TSOs are prohibited from bringing any cameras, cell phones, or other recording devices into the image viewing rooms.
- Passengers may opt out of AIT screening and undergo alternate screening procedures.
- Signs at TSA screening checkpoints that utilize AIT advise individuals that AIT screening is optional and that they may request alternate screening.

These operating protocols, coupled with the fact that TSA does not retain or in any way link AIT images to passenger records, provide ample support of TSA's compliance with both the letter and the spirit of the Privacy Act.

Religious Freedom Restoration Act (RFRA). TSA's use of AIT does not violate the RFRA.[17] As an initial matter, TSA's decision to employ AIT would not implicate the RFRA unless it is deemed to substantially burden an individual's exercise of religion.[18] But the very fact that

---

[16] See Privacy Impact Assessment - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf (July 23, 2009), updating the original PIA dated October 17, 2008.

[17] 42 U.S.C. § 2000bb, *et seq.*

[18] *See, e.g., Navajo Nation v. U.S. Forest Svc.*, 535 F.3d 1058, 1068 (9th Cir. 2008).

passengers are not required to undergo AIT screening – as noted above – necessarily means that its use at airports does not constitute a substantial burden under the RFRA.[19] Because passengers may request a pat-down as an alternative to AIT screening, TSA's use of the technology does not "force[] them to engage in conduct that their religion forbids or . . . prevent[] them from engaging in conduct their religion requires."[20] Indeed, some of the very authorities cited in your letter note that while some religious organizations have expressed concern about AIT, they also acknowledge TSA's effort to accommodate that concern by providing the option for a pat-down.[21]

Courts have long recognized that the government has a compelling interest in maintaining national security and public safety.[22] When requirements predicated on concerns of this type (*e.g.*, prison grooming requirements prohibiting long hair or beards that may facilitate smuggling of contraband, gang identity, etc., and thereby undermine prison security) are pitted against religious precepts (such as the prohibition in Rastafarian or Sunni Muslim traditions that prohibit the cutting of hair or beards), courts have consistently concluded that the requirement may in appropriate circumstances be upheld as the least restrictive means of achieving the compelling government interest.[23]

In light of these considerations, TSA's use of AIT—which serves a compelling governmental interest in security—does not implicate the RFRA. TSA's web site provides further information about how the agency addresses religious and cultural needs at the checkpoint, including the ability of travelers to request alternative, private screening by a TSO of the same gender.[24]

* * * * *

AIT machines, coupled with TSA's layered approach to security, respond to the statutory mandate and the national security imperative to screen airline passengers for both metallic and nonmetallic threats. There is widespread public acceptance of AIT screening, and TSA also provides alternative screening methods. AIT screening has proven effective in addressing ever-

---

[19] *See id.*, at 1069-70.

[20] *Henderson v. Kennedy*, 253 F.3d 12, 16 (D.C. Cir. 2001) (collecting cases).

[21] *E.g.*, your letter at notes 48 and 49.

[22] *Gillette v. United States*, 401 U.S. 437, 462 (1971); *Prince v. Massachusetts*, 321 U.S. 158, 165 (1944); *see also United States v. Acevedo-Delgado*, 167 F. Supp. 2d 477, 481 (D. Puerto Rico 2001) (noting that, in an era in which "the relative peace enjoyed by all citizens of the United States is being challenged more and more frequently by our enemies and terrorists alike," courts considering RFRA challenges "cannot simply zoom in on the concerns of [one person or group(s) of United States citizens] but it must pan back and keep the larger picture in focus [taking into account the concerns of] ALL United States citizens, citizens who are entitled to a well-trained military and national security" (internal quotations omitted)).

[23] *Jackson v. District of Columbia*, 89 F. Supp. 2d 48 (D.D.C. Mar 21, 2000) (collecting authority), *overruled on other grounds*, 254 F.3d 262 (D.C. Cir. 2001).

[24] *See* www.tsa.gov/travelers/airtravel/assistant/editorial_1037.shtm.

changing security threats, and numerous independent studies have addressed health concerns related to AIT screening. TSA has carefully considered the important Constitutional, statutory, and privacy issues associated with the deployment of AIT systems, and has taken numerous steps to address those issues in a manner that protects the rights of travelers.

We appreciate hearing the concerns expressed in your letter and hope this information is helpful.

Sincerely yours,

Francine J. Kerner

Francine J. Kerner
Chief Counsel

Attachment

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

Homeland Security

April 27, 2010

The Honorable Susan Collins
United States Senate
Washington, DC 20510

Dear Senator Collins:

Thank you for your April 12, 2010 letter regarding the imaging technology demonstrated at Amsterdam's Schiphol International Airport.

Transportation Security Administration (TSA) officials have had extensive discussions with their Dutch counterparts related to the current and future state of Advanced Imaging Technology (AIT) systems and the available automated target recognition (ATR) functionality. TSA representatives have made several visits to Schiphol to discuss the capabilities, operational effectiveness, and suitability of AIT systems—both with and without currently available ATR functionality. The Dutch have also shared testing results with us, including detection and false alarm rates for the currently deployed ATR-enabled AIT systems, and TSA has used the lessons learned from Schiphol to evaluate the use of the AIT in primary screening and determine ATR requirements for U.S. nationwide deployment. Our discussion and technical evaluation sessions with the Dutch about the current and future possibilities for ATR are ongoing,

To give you further insight, the AIT system *without* ATR functionality that is in use at Schiphol is listed on TSA's AIT Qualified Products List, and the AIT system *with* ATR functionality that is in use at Schiphol will be evaluated in a pilot. TSA has provided ATR requirements to manufacturers; once their systems are fully tested and proven to meet these requirements, TSA plans to upgrade all currently deployed systems with this new functionality.

Thank you again for your letter. I value your views on these emerging technologies, and I look forward to working with you on this and other homeland security issues. Senators Kyl and Chambliss, who co-signed your letter, will receive separate, identical responses. Should you need additional assistance, please do not hesitate to contact me at (202) 282-8203.

Yours very truly,

Janet Napolitano