

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

THE ELECTRONIC PRIVACY INFORMATION)
CENTER,)
CHIP PITTS, and BRUCE SCHNEIER,)
Petitioners,)

v.)

No. _____

JANET NAPOLITANO, in her official capacity)
as Secretary of the United States Department of)
Homeland Security, MARY ELLEN)
CALLAHAN, in her official capacity as Chief)
Privacy Officer, and THE UNITED STATES)
DEPARTMENT OF HOMELAND SECURITY,)
Respondents.)

PETITION FOR REVIEW

Petitioners the Electronic Privacy Information Center (“EPIC”), Chip Pitts, and Bruce Schneier hereby petition the Court for review of three agency actions—one failure to act, one agency Order, and one agency Rule—of the Transportation Security Administration (“TSA”), a Department of Homeland Security (“DHS”) component.

First, Petitioners petition the Court for review of the TSA’s failure to act on EPIC’s May 31, 2009 5 U.S.C. § 553(e) petition. Second, Petitioners petition the Court for review of the May 28, 2010 Order of the TSA refusing to process of

EPIC's April 21, 2010 5 U.S.C. § 553(e) petition. Third, Petitioners petition the Court for review of the TSA Rule mandating the use of "full body scanners" at airport checkpoints as primary screening; the TSA entered this Rule recently, but failed to make public the text of the Rule or its date.

Petitioner EPIC filed a Section 553(e) petition on May 31, 2009 ("the First EPIC Petition"). The First EPIC Petition notes "the [TSA's] announced plan to deploy [full body scanners] as the primary means of screening airline passengers in the United States" and urges the DHS to undertake a "a 90-day formal public rulemaking process to receive public input on the agency's use of [full body scanners]." On June 19, 2009, the DHS wrote a letter to EPIC, but failed to grant or deny EPIC's petition for the formal rulemaking concerning TSA's use of full body scanners ("the DHS Letter").

Copies of the First EPIC Petition and the DHS Letter are attached as Exhibit 1 and Exhibit 2, respectively.

On April 21, 2010 Petitioner EPIC¹ filed a Section 553(e) petition ("the Second EPIC Petition") with the TSA seeking repeal of the TSA's "rule mandating the use of body scanners at airport checkpoints as primary screening." On May 28, 2010, the TSA issued an order refusing to process the Second EPIC Petition, asserting "TSA does not interpret your letter to seek a rulemaking or to constitute a

¹ Thirty organizations, including Petitioner EPIC, filed the April 21, 2010 petition. The other twenty-nine organizations are not petitioners in the present action.

petition under 5 U.S.C. §553.” (“the TSA Order”). The TSA Order is the final administrative action in this matter, and constitutes the final agency order.

Copies of the Second EPIC Petition and the TSA Order are attached as Exhibit 3 and Exhibit 4, respectively.

The TSA recently issued, on a date unknown to Petitioners, a Rule mandating the use of “full body scanners” at airport checkpoints as primary screening. This Rule is a final administrative action, and constitutes a final agency rule.

Respectfully Submitted,



MARC ROTENBERG
JOHN VERDI

Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners

Dated: July 2, 2010

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

THE ELECTRONIC PRIVACY INFORMATION)
CENTER,)
CHIP PITTS, and BRUCE SCHNEIER,)
Petitioners,)

v.)

No. _____

JANET NAPOLITANO, in her official capacity)
as Secretary of the United States Department of)
Homeland Security, MARY ELLEN)
CALLAHAN, in her official capacity as Chief)
Privacy Officer, and THE UNITED STATES)
DEPARTMENT OF HOMELAND SECURITY,)
Respondents.)

F.R.A.P 26.1 CORPORATE DISCLOSURE STATEMENT

Petitioner the Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, or affiliate. EPIC has never issued shares or debt securities to the public.

Respectfully Submitted,



MARC ROTENBERG

JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners

Dated: July 2, 2010

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 2nd day of July, 2010, he caused one copy each of the foregoing Petition for Review and F.R.A.P. 26.1 Corporate Disclosure Statement to be served by courier on the following:

The Office of the General Counsel
U.S. Department of Homeland Security
Washington, DC 20528

Francine J. Kerner
Chief Counsel
Transportation Security Administration
U.S. Department of Homeland Security
601 South 12th St.
Arlington, VA 20598

MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners



Exhibit 1
May 31, 2009 Petition to the Department of Homeland Security
Requesting Formal Rulemaking

May 31, 2009

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

Dear Secretary Napolitano,

We the undersigned privacy, consumer rights, and civil rights organizations are writing to you regarding the Transportation Security Administration's announced plan to deploy Whole Body Imaging as the primary means of screening airline passengers in the United States. We strongly object to this change in policy and urge you to suspend the program until the privacy and security risks are fully evaluated.

Whole Body Imaging systems, such as backscatter x-ray and millimeter wave, capture a detailed image of the subject stripped naked. In this particular application, your agency will be capturing the naked photographs of millions of American air travelers suspected of no wrongdoing.

Moreover, the privacy problems with these devices have still not been adequately resolved. Even though a "chalk line" image is displayed to an operator in a remote location and even though the TSA undertook a Privacy Impact Assessment and said that the image-recording feature would be disabled, it is obvious that the devices are designed to capture, record, and store detailed images of individuals undressed.

If the public understood this, they would be outraged -- many on religious grounds -- by the use of these devices by the US government on US citizens. "The desire to shield one's unclothed figure from view of strangers, and particularly strangers of the opposite sex, is impelled by elementary self-respect and personal dignity," said the U.S. Ninth Circuit Court of Appeals in 1958. The law of privacy, according to a federal judge in California in 1976, "encompasses the individual's regard for his own dignity; his resistance to humiliation and embarrassment; his privilege against unwanted exposure of his nude body and bodily functions." Both courts were discussing dignity in prisons, even though other rights of privacy are not accorded inmates.

Further, the TSA repeatedly stated that these systems would only be used for secondary screening of passengers and only as a voluntary alternative to a pat-down search. The fact that the TSA reversed itself on the central question of whether these systems would be voluntary makes obvious the risk that the TSA will later reverse itself on the retention of images.

More must be known about the use of these devices. The American public is directly impacted by the planned use of these systems and should be given an opportunity to express its views.

We ask that the use of "Whole Body Imaging" technology undergo a 90-day formal public rulemaking process to receive public input on the agency's use of "Whole Body Imaging"

technologies.

In the interim, the agency should suspend the use of Whole Body Imaging to screen all travelers. Individuals who are asked to undergo secondary screening must be fully informed of their right to alternative secondary screening options. Not native English speaking passengers must be informed via multi-lingual oral and written formats that include an image comparable to the size of the image that will be produced by the Whole Body Image technology. Passengers should also have alternatives to the Whole Body Imaging option for secondary screening such as a pat down, or physical search of carry-on bags.

The TSA should also investigate less invasive means of screening airline passengers. The expense of the technology to taxpayers should be considered in light of other less costly means of creating a secure air travel experience.

Finally, we seek a full investigation of the medical and health implications of repeated exposure to Whole Body Imaging technology. The frequency of air travel, medical conditions such as pregnancy, and chronic health conditions, and repeated exposure of TSA and airport personnel stationed in the vicinity of the technology should be assessed. Age, gender, pre-existing medical conditions, and other factors should be evaluated and medical recommendations developed regarding the use of any Whole Body Imaging system.

Sincerely,

American Association of Small Property Owners
American Civil Liberties Union
Americans for Democratic Action
Calegislation
Center for Democracy and Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Constitution Project
Consumer Action
Consumer Federation of America
Consumer Travel Alliance
Consumer Watchdog
Cyber Privacy Project
Discrimination and National Security Initiative
Electronic Privacy Information Center
Fairfax County Privacy Council
Feminists for Free Expression
Gun Owners of America
Identity Project (PapersPlease.org)
Liberty Coalition
National Center for Transgender Equality
National Workrights Institute
Pain Relief Network

Patient Privacy Rights
Privacy Activism
Privacy Journal
Privacy Rights Clearinghouse
Privacy Times
The Multiracial Activist
The Rutherford Institute
Transgender Law Center
U.S. Bill of Rights Foundation
Woodhull Freedom Foundation
World Privacy Forum

Exhibit 2

June 19, 2009 Letter from the Transportation Security Administration

JUN 19 2009



**Transportation
Security
Administration**

Ms. Lillie Coney
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave, NW
Suite 200
Washington, DC 20009

Dear Ms. Coney:

Thank you for your letter of May 31, 2009, to Secretary Janet Napolitano on behalf of 24 groups regarding privacy concerns associated with the Transportation Security Administration (TSA) Whole Body Imaging (WBI) program. I would like to take this opportunity update you on TSA's WBI program and the privacy protections that are accompanying the deployment of WBI equipment.

As you know, whole body imaging is an umbrella term used to describe a number of technologies that enable TSA to detect prohibited items that may be concealed under clothing without a physical search of a passenger. WBI is a key component of TSA efforts to address evolving security threats, including non-metallic threat items. To date, 19 airports across the nation are using WBI technology, and at six of those airports, WBI is being used in primary screening. At all locations, individuals who do not want to go through WBI screening may decline in favor of a pat-down, whether in primary or secondary screening.

TSA is committed to preserving privacy in its security programs and believes strongly that the WBI program accomplishes that through a screening protocol that ensures complete anonymity for the individual undergoing the WBI scan. This is achieved by physically separating the officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The WBI scanned images cannot be stored or retained, pursuant to a factory setting that cannot be changed by the operator. Cameras and cell phones are not allowed in the viewing room under any circumstances. Further anonymity protection is achieved by a filter on the scanned image that blurs the face of the individual who was scanned. TSA has not deviated from these operational protocols, first published in the Privacy Impact Assessment for WBI in January 2008 prior to the first devices being operated in the WBI pilot. While we believe that these privacy protections are robust, we also believe that improvements in WBI technology will allow us to add even more privacy protections in the future while continuing to maintain the effectiveness of these systems to detect threat items.

From the outset of the WBI program, TSA has worked to inform the public on WBI screening and to listen to public reaction to the technology. These efforts are not static:

we continue to listen to the public, and we constantly look for ways to improve our outreach and education. TSA outreach has included briefings to the Privacy Coalition in March 2007 and again in December 2008. Indeed, it was a comment specifically from you at the March 2007 meeting that prompted signage being placed directly on the WBI devices instead of only being made available in a brochure. Recently, we improved the signage at the entrance to the passenger screening queue. In the near future, we also will be adding WBI information on the video screens at checkpoints with WBI screening. In October 2007, TSA offered demonstrations of the technology to news organizations and to privacy groups, including three groups that signed your letter (American Civil Liberties Union, EPIC, and Center for Democracy and Technology). The TSA web site has information on WBI screening at www.tsa.gov/approach/tech/body_imaging.shtm. The TSA blog, one of the most heavily trafficked blogs in the Federal government (third behind only the White House and the Congressional Budget Office blogs), has made repeated posts on the WBI program, and TSA considered views expressed in several hundred comments to the posts as well as reaction to articles in the news and travel media. TSA also considered international reaction to the deployment of WBI by other governments at foreign airports.

Finally, with respect to health concerns, the energy (both x-ray and millimeter wave) generated by the WBI devices are only a small fraction of the energy that individuals are exposed to every day. The x-ray energy is equivalent to 2 minutes of flight at altitude, or the energy that every living thing is exposed to in a single day at ground level, while the millimeter wave energy is equivalent to 1/100,000 of the energy permitted by the FCC for cell phones.

We appreciate hearing the concerns expressed in your letter and hope this information is helpful. If you need additional assistance, please contact Peter Pietra, Director, Privacy Policy & Compliance, at TSAprivacy@dhs.gov.

Sincerely yours,



Gale D. Rossides
Acting Administrator

Exhibit 3
April 21, 2010 Petition to the Department of Homeland Security
Requesting Stay of Agency Rule

April 21, 2010

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

Chief Privacy Officer Mary Ellen Callahan
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Petition for Suspension of TSA Full Body Scanner Program

Dear Secretary Napolitano and Ms. Callahan,

We the undersigned privacy, consumer rights, and civil rights organizations hereby petition¹ the Department of Homeland Security (“DHS”) and its component, the Transportation Security Administration (“TSA”) to suspend the ongoing deployment of the TSA’s Full Body Scanner (“FBS”) program. The TSA program uses FBS devices (also called “whole body imaging” machines) to screen air travelers in the United States.

We strongly object to the TSA’s use of full body scanners as primary, mandatory screening at security checkpoints. On May 31, 2009, twenty-four privacy and civil liberties groups² wrote to the DHS requesting, *inter alia*, that the DHS conduct “a 90-day formal public rulemaking process to receive public input on the agency’s use of ‘Whole Body Imaging’ technologies.”³ The DHS failed to initiate a rulemaking. Instead, the TSA recently announced its intent to deploy approximately one thousand additional FBS devices to American airports.⁴ Although the TSA failed to conduct a formal rulemaking, it is clear that the TSA has established a rule mandating the use of body scanners at airport checkpoints as primary screening. EPIC petitions the TSA to repeal that rule, and suspend the Full Body Scanner program.

The deployment of Full Body Scanners in US airports, as currently proposed, violates the U.S. Constitution, the Religious Freedom Restoration Act (“RFRA”), the Privacy Act of 1974 (“Privacy Act”), and the Administrative Procedures Act (“APA”). As described below, the FBS program effectively subjects all air travelers to unconstitutionally intrusive searches that are disproportionate and for which the TSA lacks any suspicion of wrongdoing. The FBS Program also violates the RFRA because it requires those of sincerely held religious beliefs to be subject

¹ The undersigned file this petition pursuant to 5 U.S.C. § 553(e), which requires that “[e]ach agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule.”

² The May 31, 2009 letter signatories include many of the undersigned groups.

³ Letter from EPIC and thirty-three organizations to Secretary Janet Napolitano, U.S. Dep’t. of Homeland Security (May 31, 2009), *available at* epic.org/privacy/airtravel/backscatter/Napolitano_ltr-wbi-6-09.pdf.

⁴ U.S. Government Accountability Office, Testimony Before the House Subcommittee on Transportation Security and Infrastructure Protection, *TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Other Areas of Aviation Security Remain*, Mar. 17, 2010 at 1 *available at* <http://www.gao.gov/new.items/d10484t.pdf>.

to offensive intrusions by government officials. The program violates the Privacy Act because the system gathers personally identifiable information—a detailed and unique image of the human body easily associated with a particular airline ticket—yet the TSA failed to publish a System of Records Notice. The TSA Chief Privacy Office violated its statutory obligations to ensure that new technologies “sustain and do not erode” the privacy of Americans when it effectively approved the program.

Further, substantial questions have been raised about the effectiveness of the devices, including whether they could detect powdered explosives—the very type of weapon used in the December 25, 2009 attempted airliner bombing. The full body scanning program is enormously expensive, costing taxpayers at least \$2.4 billion dollars. There are less intrusive and less costly techniques available to address the risk of concealed explosives on aircrafts. For example, last week, U.S. Senators asked the DHS to evaluate alternative technologies that could “address many of the privacy concerns raised by the scanners DHS is currently testing.”⁵

I. The Agency is Undertaking an Aggressive Plan to Deploy Full Body Scanners in US Airports without regard to Effectiveness, Traveler Complaints, Privacy Risks, or Religious Objections

A) The Plan to Deploy Approximately One Thousand Full Body Scanners to American Airports

The TSA operates Full Body Scanners at airports throughout the United States.⁶ The TSA uses two types of FBS devices: backscatter x-ray and millimeter wave.⁷ Both types of FBS devices can capture, store, and transfer⁸ detailed, three-dimensional images of individuals’ naked bodies.⁹ Experts have described full body scans as “digital strip searches.”¹⁰ The images captured by FBS devices can uniquely identify individual air travelers. The TSA uses FBS devices to search air travelers as they pass through the TSA’s airport security checkpoints.¹¹

FBS devices are currently deployed at: Albuquerque International Sunport Airport, Boston Logan International Airport, Chicago O’Hare International Airport, Cincinnati/Northern Kentucky International Airport, Hartsfield-Jackson Atlanta International Airport, Baltimore/Washington International Thurgood Marshall Airport, Denver International Airport,

⁵ Letter from Sen. Susan Collins, Sen. Saxby Chambliss, and Sen. Jon Kyl to Secretary Janet Napolitano, U.S. Dep’t. of Homeland Security (Apr. 12, 2010) *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MinorityNews&ContentRecord_id=f8689ee7-5056-8059-767f-091debe8eae4.

⁶ TSA, *TSA: Imaging Technology*, http://www.tsa.gov/approach/tech/imaging_technology.shtm (last visited Apr. 15, 2010).

⁷ *Id.*

⁸ TSA Office of Security Technology System Planning and Evaluation, *Procurement Specification for Whole Body Imager Devices for Checkpoint Operations*, Sept. 23, 2008 (“TSA Procurement Specifications Document”) at 5, *available at* http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf (stating “When in Test Mode, the WBI: shall allow exporting of image data in real time; ... shall provide a secure means for high-speed transfer of image data; [and] shall allow exporting of image data (raw and reconstructed)”).

⁹ E.g. Wikipedia, Backscatter X-ray, http://en.wikipedia.org/wiki/Backscatter_X-ray; L3, L3 Composite, <http://www.sds.l-3com.com/products/i/L-3%20composite%20300dpi.jpg>.

¹⁰ Privacy Coalition, *Stop Digital Strip Searches*, <http://www.stopdigitalstripsearches.org/>.

¹¹ *Supra* note 5.

Dallas/Fort Worth International Airport, Detroit Metro Airport, Indianapolis International Airport, Jacksonville International Airport, Kansas City International Airport, McCarran International Airport, Los Angeles International Airport, Miami International Airport, Phoenix Sky Harbor International Airport, Raleigh-Durham International Airport, Richmond International Airport, Ronald Reagan Washington National Airport, San Francisco International Airport, Salt Lake City International Airport, Tampa International Airport, and Tulsa International Airport.¹²

In March 2010, the TSA began deploying additional FBS devices in American airports.¹³ In March 2010, the TSA announced its decision to further deploy approximately one thousand additional FBS devices to American airports.¹⁴ As a matter of pattern, practice and policy, the TSA requires air travelers to submit to FBS searches once they have entered the security zone in airports equipped with FBS devices.¹⁵ As a matter of pattern, practice and policy, the TSA employs FBS searches as a primary search of air travelers in airports equipped with FBS devices.¹⁶ As a matter of pattern, practice and policy, the TSA does not offer air travelers a meaningful alternative to FBS searches in airports equipped with FBS devices.¹⁷ As a matter of pattern, practice and policy, the TSA does not offer air travelers with religious objections to Full Body Scanning a meaningful alternative to FBS searches in airports equipped with FBS devices.¹⁸

B) The TSA's Full Body Scanner Program Collects and Retains Detailed Personal Information About Air Travelers

The TSA requires air travelers to disclose their full name, birth date, and gender when purchasing a ticket.¹⁹ The TSA obtains additional information about air travelers from airlines, government agencies, and other third parties. The TSA collects and stores this information, linking it to air travelers' itineraries. The TSA requires air travelers to submit to searches of their

¹² *Supra* note 5.

¹³ U.S. Government Accountability Office, Testimony Before the House Subcommittee on Transportation Security and Infrastructure Protection, *TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Other Areas of Aviation Security Remain*, Mar. 17, 2010 at 1 available at <http://www.gao.gov/new.items/d10484t.pdf>.

¹⁴ *Id.*

¹⁵ Air Traveler Complaints to the TSA at 45, <http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf> (air traveler stated that "when he requested an alternative screening, the TSA screeners interrogated and laughed at him."); at 53 (air traveler "was told to go in this machine and ... was not told that this machine would do a full body scan. I did not know what I went thru[sic] until today, when I read the article on line.").

¹⁶ *Id.* at 67 ("I am outraged and angry that what was supposed to be a 'pilot' for the millimeter scan machines has now become MANDATORY at SFO. I have transited through the International A terminal boarding area several times over the past few months and TSA has shut down all lanes other than the scanner.") (emphasis in original).

¹⁷ *Id.* at 62, ("I was picked to go through the new body scanner machine ... When I looked around, I noticed that there were only women who were 'told' to go through this machine, there were no men. I would have refused, but didn't realize that I could until I read up on the scanner."); at 65 ("I was asked/forced into this [body scanner] at BWi airport on 6/30/09"); at 69 ("the TSA guard sent my wife and I through the new X-Ray machine ... A guard did not give us a choice."); at 69 ("I am 70 years old. [At BWI, I] went through the metal detector ... with apparently no problems, I proceeded to collect my belongings ... but was stopped [for a body scan]. I was never told why I had to do this, had no idea what was being done."); at 72 ("[I] decided to opt out [of a FBS scan]. My family and I were then subjected to a punitive pat-down search (they went over me three times) that would have been considered sexual assault in any other context.").

¹⁸ *Id.* at 92 (describing mandatory body scan and subsequent patdown of devout Muslim air traveler).

¹⁹ TSA, *Secure Flight Update*, Jul. 15, 2009, <http://www.tsa.gov/blog/2009/07/secure-flight-update.html>

bodies and carry-on luggage at TSA airport security checkpoints.²⁰ The TSA requires that air travelers present a boarding pass and government-issued photo identification card at airport security checkpoints.²¹ The boarding pass displays air travelers' full names, travel itineraries, and bar codes containing machine-readable versions of travelers' personal information.²² As a matter of pattern, practice and policy, the TSA visually matches air travelers' photo ID cards with their boarding passes when travelers pass through airport security checkpoints.²³ As a matter of pattern, practice and policy, the TSA scans air traveler's boarding passes, collecting air travelers' personal information, when travelers pass through airport security checkpoints that are equipped with paperless boarding pass scanners.²⁴

As described above, the TSA employs full body scanners to search air travelers at airport security checkpoints.²⁵ As described above, FBS devices can capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies.²⁶ As a matter of pattern, practice, and policy, the TSA requires air travelers to possess and often display boarding passes contemporaneous with FBS searches. The TSA is therefore able to associate a specific FBS image with the full name, birth date, gender, and travel itinerary of the scanned traveler. The TSA failed to publish a "system of records notice" concerning the FBS Program in the Federal Register.

C) The TSA Misrepresents the Full Body Scan Program

The TSA claims that FBS devices cannot capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies.²⁷ In fact, the FBS devices employed by the TSA can capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies, as per the TSA's own requirements.²⁸ The TSA claims that FBS searches are "optional."²⁹ In fact, as a matter of pattern, practice and policy, the TSA does not offer air travelers a meaningful alternative to FBS searches in airports equipped with FBS devices.³⁰

²⁰ TSA, *TSA Travel Assistant*, <http://www.tsa.gov/travelers/airtravel/screening/index.shtm>; TSA, *3-1-1 on Air Travel*, <http://www.tsa.gov/311/index.shtm>.

²¹ TSA, *The Screening Experience*, http://www.tsa.gov/travelers/airtravel/assistant/editorial_1044.shtm.

²² Wikipedia, *Boarding Pass*, http://en.wikipedia.org/wiki/Boarding_pass; *see also* Wikipedia, *Bar Coded Boarding Pass*, http://en.wikipedia.org/wiki/Bar_Coded_Boarding_Pass

²³ TSA, *TSA Announces Enhancements to Airport ID Requirements to Increase Safety*, Jun. 23, 2008, http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm.

²⁴ TSA, *Paperless Boarding Pass Pilot*, http://www.tsa.gov/approach/tech/paperless_boarding_pass_expansion.shtm.

²⁵ *Supra* note 5.

²⁶ *Supra* notes 7-8.

²⁷ *Supra* note 5 (claiming "The image cannot be stored, transmitted or printed, and is deleted immediately once viewed.").

²⁸ *Supra* notes 7-8.

²⁹ *Supra* note 5 (claiming "Advanced imaging technology screening is **optional for all passengers.**"[emphasis in original]).

³⁰ *Supra* note 16; *see also supra* note 5 (stating "passengers who do not wish to utilize this screening will receive an equal level of screening, including a physical pat-down.").

In 2007, the TSA stated that FBS searches would not be mandatory for passengers, but rather “a voluntary alternative to a pat-down during secondary screening.”³¹ In fact, as a matter of pattern, practice and policy, the TSA employs FBS searches as a primary search of air travelers in airports equipped with FBS devices.³² The TSA has claimed that “a security algorithm will be applied to the image to mask the face of each passenger.”³³ In fact, the FBS devices employed by the TSA can capture images without any security algorithm and without masking the face of each passenger.³⁴

The TSA claims that air travelers prefer FBS searches.³⁵ In fact, hundreds of air travelers have lodged objections with the TSA, alleging a host of law and policy violations arising from the TSA’s FBS searches.³⁶ Air travelers object to the invasiveness of the FBS searches.³⁷ Air travelers state that they are not informed when they undergo a FBS search, or of a pat-down alternative.³⁸ Air travelers object to the use of FBS devices to search vulnerable individuals, including children and pregnant women.³⁹ Pregnant air travelers objected to the TSA’s FBS search after the TSA scanned them without identifying the machine or informing them of how it operates.⁴⁰

D) Full Body Scanner Technology is Flawed

The FBS devices employed by the TSA are not designed to detect powdered explosives.⁴¹ The FBS devices employed by the TSA are not designed to detect powdered pentaerythritol

³¹ *TSA Tests Second Passenger Imaging Technology at Phoenix Sky Harbor Airport*, Transportation Security Administration, October 11, 2007 available at http://www.tsa.gov/press/releases/2007/press_release_10112007.shtm; see also *X-Ray Backscatter Technology and Your Personal Privacy*, <http://web.archive.org/web/20080112014635/http://www.tsa.gov/research/privacy/backscatter.shtm> (archived January 12, 2008) (stating “Backscatter is a voluntary option for passengers undergoing secondary screening as an alternative to the physical pat down procedures”).

³² *Supra* note 15.

³³ TSA, *TSA Tests Second Passenger Imaging Technology at Phoenix Sky Harbor Airport*, Oct. 11, 2007, http://www.tsa.gov/press/releases/2007/press_release_10112007.shtm.

³⁴ TSA Systems Engineering Branch, *Operational Requirements Document, Whole Body Imager Aviation Applications*, July 2006, (“TSA Operational Requirements Document”) at 8 available at http://epic.org/open_gov/foia/TSA_Ops_Requirements.pdf (stating “the WBI shall provide ten selectable levels of privacy.”); TSA Procurement Specifications Document at 5 (Enabling and disabling of image filtering shall be modifiable by users as defined in the User Access Levels and Capabilities appendix).

³⁵ *Supra* note 5 (claiming “Many passengers prefer advanced imaging technology. In fact, over 98 percent of passengers who encounter this technology during TSA pilots prefer it over other screening options.”).

³⁶ Air Traveler Complaints to the TSA available at <http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf>, <http://epic.org/privacy/airtravel/backscatter/EPIC2.pdf>, <http://epic.org/privacy/airtravel/backscatter/EPIC3.pdf>, <http://epic.org/privacy/airtravel/backscatter/EPIC4.pdf>, <http://epic.org/privacy/airtravel/backscatter/EPIC5.pdf>.

³⁷ Air Traveler Complaints to the TSA at 19, 24, 27, 28, 37 available at <http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf> (complaints stating that body scanners are “a disgusting violation of civil liberties and privacy,” “for a bunch of peeping toms,” “unconstitutional,” “intrusive and ridiculous” and “a joke.”).

³⁸ *Supra* note 16.

³⁹ *E.g.* TSA Traveler Complaints at 14, 21, 25, 85.

⁴⁰ TSA Traveler Complaints at 159; TSA Traveler Complaints at 11-12, available at <http://epic.org/privacy/airtravel/backscatter/EPIC2.pdf>.

⁴¹ TSA Procurement Specifications Document at 4 (requiring body scanners to detect liquid, but not powdered, material.); see also Jane Merrick, *Are Planned Airport Scanners Just a Scam?*, *The Independent* (UK), Jan. 3 2010

tetranitrate (“PETN”)—the explosive used in the attempted December 25, 2009 bombing of Northwest Airlines flight 253.⁴² The FBS devices employed by the TSA have profound technical flaws that allow the machines to be breached and create the risk that sensitive traveler images could be leaked.

The FBS devices employed by the TSA run Windows XPe, which contains security vulnerabilities.⁴³ The FBS devices employed by the TSA are designed to transfer information via highly transportable and easily concealable USB devices.⁴⁴ The FBS devices employed by the TSA are equipped with Ethernet network interfacing capabilities that are vulnerable to security threats.⁴⁵ The FBS devices employed by the TSA permit TSA employees to disable built-in “privacy safeguards.”⁴⁶

II. The Plan to Deploy Full Body Scanners is Widely Opposed, Violates the Fourth Amendment, and Several Federal Acts, including the Religious Freedom and Restoration Act, The Administrative Procedures Act, and the Privacy Act

A) Religious Leaders Object to Full Body Scanners

On February 20, 2010, Pope Benedict XVI objected to FBS searches because they fail to preserve the integrity of individuals.⁴⁷ Agudath Israel, an Orthodox Jewish umbrella group, objects to FBS searches, calling the devices “offensive, demeaning, and far short of acceptable norms of modesty” within Judaism and other faiths.⁴⁸ On February 9, 2010, The Fiqh Council of North America objected to body scanners, announcing that “general and public use of such

available at <http://www.independent.co.uk/news/uk/home-news/are-planned-airport-scanners-just-a-scam-1856175.html> (noting that body-scanners “have been touted as a solution to the problem of detecting ... liquids, chemicals or plastic explosive. But Ben Wallace, the Conservative MP, who was formerly involved in a project by a leading British defence research firm to develop the scanners for airport use, said trials had shown that such low-density materials went undetected.”).

⁴² *Id*; see also Kenneth Chang, *Explosive on Flight 253 Is Among Most Powerful*, N.Y. Times, Dec. 27, 2009 *available at* http://www.nytimes.com/2009/12/28/us/28explosives.html?_r=1.

⁴³ TSA Contract HSTS04-06-R-CTO046 with L3 (“TSA Contract with L3”) at 27 *available at* http://epic.org/open_gov/foia/TSA_Millwave_Contract.pdf; See Konstantin Morozov, White Paper, *Best Practices for Protecting Windows XP Embedded Devices* at 4, *available at*

<http://www.dstacom.au/DSTeupload/protectingxpedevices.pdf> (“In general, malware does not affect Windows Mobile devices, such as Smartphone and Pocket PCs, and other devices based on Windows CE, as much as it impacts devices running Windows XP Embedded. This is because Windows XP Embedded is based on the same feature binaries as Windows XP Professional and thus has similar vulnerabilities that can be exploited.”); Brian Krebs, *Windows Security Flaw is ‘Severe,’* Washington Post, Dec. 29, 2005, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/29/AR2005122901456.html>.

⁴⁴ TSA Procurement Specifications Document at 10 (“the WBI shall provide capabilities for data transfers via USB devices.”).

⁴⁵ TSA Procurement Specifications Document at 7; TSA Operational Requirements Document at 10-11.

⁴⁶ TSA Procurement Specifications Document at 5 (Enabling and disabling of image filtering shall be modifiable by users as defined in the User Access Levels and Capabilities appendix).

⁴⁷ Catholic News Agency, *Benedict XVI Urges Airports to Protect Integrity of Travelers*, Feb. 20, 2010, http://www.catholicnewsagency.com/news/benedict_xvi_calls_for_airports_to_protect_integrity_of_travelers/.

⁴⁸ Omar Sacirbey, *Jews, Muslims Worry Body Scanners Violate Religious Laws*, Mar. 3, 2010, http://www.religionnews.com/index.php?/mstext/jews_muslims_say_body_scanners_violate_religious_laws/.

scanners is against the teachings of Islam, natural law and all religions and cultures that stand for decency and modesty.”⁴⁹

American air travelers have filed objections with the TSA on religious grounds.⁵⁰ On February 19, 2010, two Muslim women refused to submit to a body scan at the Manchester Airport, forfeiting their tickets to Pakistan rather than undergo the scan.⁵¹ In March 2010, a six-member Pakistani parliamentary delegation from the Federally Administered Tribal Areas refused to submit to full body scanning at the Washington Dulles International Airport, stating it was an insult to parliamentarians of a sovereign country.⁵² Instead, they ended their visit to the US and returned to Pakistan.⁵³

B) The TSA’s Full Body Scanner Program Violates the Fourth Amendment and the RFRA

The TSA’s FBS program subjects air travelers to unreasonable searches. The program requires air travelers to submit to a uniquely invasive search without any suspicion that particular individuals have engaged in wrongdoing. Courts have upheld some invasive airport checkpoint searches, but typically on the basis that the searches are part of a progressively escalating series of screenings.⁵⁴ Full Body Scanners are part of no such program. Instead, they employ the intrusive, degrading digital strip search as mandatory, primary screening.

The TSA program particularly burdens devout air travelers. As noted above, many religious leaders condemn digital strip searches as incompatible with religious tenets. Yet the TSA’s practice of requiring Full Body Scans as mandatory, primary screening leaves religious travelers without a meaningful alternative. The program violates RFRA because the TSA’s interest in conducting a Full Body Scan is limited, particularly given that the scanners’ are not designed to detect powdered explosives. Further, Full Body Scanners are not the least restrictive means of furthering the TSA’s interest in safeguarding air travel.⁵⁵

⁴⁹ Fiqh Council of North America, *Home*, <http://www.fiqhcouncil.org/> (last visited April 15, 2010) (stating “a general and public use of such scanners is against the teachings of Islam, natural law and all religions and cultures that stand for decency and modesty.”).

⁵⁰ *E.g.* Air Traveler Complaints to the TSA *available at* http://epic.org/privacy/airtravel/backscatter/3-2_Interim_Response.pdf.

⁵¹ Will Pavia, *Muslim Woman Refuses Body Scan at Airport*, Mar. 3, 2010, *The Times (UK)* *available at* <http://www.timesonline.co.uk/tol/travel/news/article7048576.ece>.

⁵² Press TV, *Pakistan MPs End US Visit to Protest Body Scanners*, Mar. 7, 2010 <http://www.presstv.ir/detail.aspx?id=120286§ionid=351020401>.

⁵³ *Id.*

⁵⁴ *E.g. United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2006) (finding airport searches reasonable because they “were well-tailored to protect personal privacy, escalating in invasiveness only after a lower level of screening disclosed a reason to conduct a more probing search. The search began when Hartwell simply passed through a magnetometer. ... Only after Hartwell set off the metal detector was he screened with a wand. ... And only after the wand detected something solid on his person, and after repeated requests that he produce the item, did the TSA agents ... reach into his pocket.”).

⁵⁵ *Supra* note 5 (observing that passive scanners “incorporate auto-detection technology that addresses many of the privacy concerns raised by the scanners DHS is currently testing, while also appearing to provide a highly effective scan.”)

C) The TSA's Full Body Scanner Program Violates the Privacy Act

As described above, the TSA's Full Body Scanner Program creates a group of records containing air travelers' personally-identifiable information. The group of records is under the control of the TSA, and the TSA can retrieve information about air travelers by name or by some identifying number, symbol, or other identifying particular assigned to the individual. The TSA's FBS program has created and/or revised a "system of records" under the Privacy Act. The TSA unlawfully failed to publish a "system of records notice" in the Federal Register, and otherwise failed to comply with its Privacy Act obligations concerning the FBS Program.

D) The TSA's Full Body Scanner Program Violates the Administrative Procedures Act

The DHS Chief Privacy Officer has a statutory obligation to "assur[e] that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."⁵⁶ The DHS Chief Privacy Officer has a statutory obligation to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."⁵⁷ The DHS Chief Privacy Officer has a statutory obligation to "conduct[] a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected."⁵⁸

The DHS Chief Privacy Office prepared an inadequate Privacy Impact Assessment of the TSA's FBS test program.⁵⁹ The inadequate assessment, which was subsequently revealed through Freedom of Information Act litigation, failed to identify numerous privacy risks to air travelers. The DHS Chief Privacy Office failed to prepare any Privacy Impact Assessment concerning the TSA's current FBS program. The TSA's current FBS program is materially different from the TSA's FBS test program. The TSA's use of full body scanners fails to comply with the Privacy Act. The program erodes, and does not sustain, privacy protections relating to the use, collection, and disclosure of air traveler's personal information.

III. Petition for Relief: Suspend Purchase, Deployment, and Operation of Full Body Scanners

The undersigned hereby request and petition the DHS and TSA for relief. As set forth above, the TSA's Full Body Scanner program violates the Fourth Amendment, the RFRA, the Privacy Act, and the APA. We request that the DHS and TSA immediately suspend purchase and deployment of Full Body Scanners to American airports. In addition, we request that the DHS and TSA cease operation of already-deployed Full Body Scanners as primary screening.

⁵⁶ 6 U.S.C. § 142(1) (2009).

⁵⁷ 6 U.S.C. § 142(2) (2009).

⁵⁸ 6 U.S.C. § 142(4) (2009).

⁵⁹ DHS, *Privacy Impact Assessment for TSA Whole Body Imaging* (Oct. 17, 2008) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf; see also DHS, *Privacy Impact Assessment Update for TSA Whole Body Imaging* (Jul. 23, 2009) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf.

Sincerely,

Electronic Privacy Information Center
American Civil Liberties Union
American Policy Center
Asian American Legal Education and Defense Fund
Bill of Rights Defense Committee
Calegislation
Campaign for Liberty
Center for Financial Privacy and Human Rights
Center for the Study of Responsive Law
Citizen Outreach
Consumer Federation of America
Consumer Travel Alliance
Consumer Watchdog
Council on American Islamic Relations
Cyber Privacy Project
Essential Information
Government Accountability Project
The Identity Project
Liberty Coalition
Muslim Legal Fund of America
National Center for Transgender Equality
National Workrights Institute
Patient Privacy Rights
Privacy Activism
Privacy Rights Clearinghouse
Public Citizen Litigation Group
Republican Liberty Caucus
Rutherford Institute
U.S. Bill of Rights Foundation
World Privacy Forum

Exhibit 4
May 28, 2010 Letter from the Transportation Security Administration



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,

A handwritten signature in black ink that reads "Francine J. Kerner". The signature is written in a cursive, flowing style.

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,

A handwritten signature in black ink, appearing to read "Janet Napolitano", with a horizontal line extending to the right.

Janet Napolitano