No. 10-1157

ORAL ARGUMENT NOT YET SCHEDULED

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

THE ELECTRONIC PRIVACY INFORMATION CENTER,
CHIP PITTS, BRUCE SCHNEIER, and NADHIRA AL-KHALILI
Petitioners,

v.

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

OPENING BRIEF FOR PETITIONERS ELECTRONIC PRIVACY INFORMATION CENTER, CHIP PITTS, BRUCE SCHNEIER, and NADHIRA AL-KHALILI

MARC ROTENBERG
JOHN VERDI
GINGER MCCALL[*]
Electronic Privacy Information
Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

[*] Ms. McCall is admitted to practice in Pennsylvania. Admission to the District of Columbia bar is pending. EPIC Appellate Advocacy Fellow Conor Kennedy and EPIC Domestic Security Fellow Amie Stepanovich participated in the preparation of this brief.

Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier

NADHIRA AL-KHALILI
453 New Jersey Ave., South East
Washington, DC 20003
(202) 488-8787
Pro se Petitioner

CERTIFICATE AS TO PARTIES, RULINGS AND RELATED CASES

Pursuant to F.R.A.P. 26.1, and D.C. Cir. Rules 27(a)(4) and 28(a)(1)(A), Petitioners certify as follows:

A. Parties

Petitioners are the Electronic Privacy Information Center ("EPIC"), Chip Pitts, Bruce Schneier, and Nadhira Al-Khalili. EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, nor affiliate. EPIC has never issued shares or debt securities to the public. 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.

Chip Pitts is the immediate past-President of the Bill of Rights Defense Committee, a Lecturer at Stanford Law School, and former Chairman of Amnesty International USA. Bruce Schneier is an internationally renowned security technologist and author. Both Mr. Pitts and Mr. Schneier are members of the EPIC Advisory Board. Mr. Schneier is also a member of the EPIC Board of Directors. Nadhira Al-Khalili is Legal Counsel for the Council on American-Islamic Relations ("CAIR").

Respondents are Janet Napolitano, in her official capacity as Secretary of the U.S. Department of Homeland Security, Mary Ellen Callahan, in her official

capacity as Chief Privacy Officer of the U.S. Department of Homeland Security, and the U.S. Department of Homeland Security ("DHS").

B. Rulings Under Review

Petitioners seek review of three agency actions—a failure to act on a petition, an agency Order, and an agency Rule—of the Transportation Security Administration ("TSA"), a 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 EPIC's April 21, 2010 5 U.S.C. § 553(e) petition. Third, Petitioners petition the Court for review of the TSA Rule effectively mandating the use of "full body scanners" at airport checkpoints as primary screening; the TSA entered this Rule in the spring of 2009, but failed to make public the text of the Rule or its date. No Federal Register citations exist concerning the three agency actions.

C. Related Cases

Petitioners previously filed a motion for emergency stay before this court, which the court construed as a motion for injunction. This court ordered that the motion be denied and determined that "Petitioners have not satisfied the stringent standards required for an injunction pending judicial review." *Electronic Privacy Information Center v. Dept. of Homeland Security*, No. 10-1157 (D.C. Cir. Sept. 1,

2010) (order denying motion to stay case). The Court further directed the Clerk to "enter a briefing schedule and to schedule oral argument on the first appropriate date following the completion of briefing." *Id.*

The case on review is not before any other court.

/s/ Marc Rotenberg
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier

/s/ Nadhira Al-Khalili
NADHIRA AL-KHALILI
453 New Jersey Ave., South East
Washington, DC 20003
(202) 488-8787
Pro se Petitioner

Dated: November 1, 2010

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

THE ELECTRONIC PRIVACY INFORMATION CENTER, CHIP PITTS, BRUCE SCHNEIER, and NADHIRA AL-KHALILI Petitioners, v. 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.	)	No. 10-1157

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. EPIC 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,

/s/ Marc Rotenberg
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier

Dated: November 1, 2010

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Authorities upon which we chiefly rely are marked with asterisks.

Administrative Record

Miscellaneous

GLOSSARY

AIT	Advanced Imaging Technology
AR	Administrative Record
AALEDF	Asian American Legal Education and Defense Fund
APA	Administrative Procedure Act
CAIR	Council on American Islamic Relations
DHS	U.S. Department of Homeland Security
EPIC	Electronic Privacy Information Center
FBS	Full Body Scanner
GAO	Government Accountability Office
MLFA	Muslim Legal Fund of America
RFRA	Religious Freedom Restoration Act
TSA	Transportation Security Administration
TSO	Transportation Security Officer
WBI	Whole Body Imaging

JURISDICTIONAL STATEMENT

Any person with "a substantial interest" in an order "with respect to [the TSA's] security duties and powers" may "apply for review of the order by filing a petition for review in the United States Court of Appeals for the District of Columbia Circuit." 49 U.S.C. § 46110(a). The Circuit courts have "exclusive jurisdiction to affirm, amend, modify, or set aside any part of the order and may order the [TSA] to conduct further proceedings." 49 U.S.C. § 46110(c); *Tooley v. Napolitano*, 556 F.3d 836, 840-41 (D.C. Cir. 2009).

Petitioners have a substantial interest in the TSA rule and the TSA order at issue in this suit. The TSA body scanner rule effectively mandates the use of body scanners at airport checkpoints for all travelers. The May 28, 2010 TSA order ignored EPIC's April 21, 2010 5 U.S.C. § 553(e) petition concerning the TSA rule. EPIC has both a well-established interest in agency practices that implicate the privacy right of travelers and a specific interest, as set out in the petitions, concerning the TSA body scanner rule. Petitioners Pitts and Schneier are frequent travelers who were subjected to full body scanner searches by the TSA. Petitioner Al-Khalili has religious objections to undergoing Full Body Scans and is a frequent traveler who will undoubtedly be subjected to Full Body Scans pursuant to the TSA body scanner rule.

The TSA established this Administrative Procedure Act rule ("the TSA Rule") recently, but failed to make public the text of the rule or its date. The TSA Rule is a final administrative action, and constitutes a final agency rule.

STATEMENT OF ISSUES FOR REVIEW

1. Whether the TSA and respondents violated the Administrative Procedure Act, 5 U.S.C. § 553(e), in failing to act on EPIC's May 31, 2009 petition ("the First EPIC Petition"), which urged a public rulemaking on a substantial change in agency practice that made body scanners the primary screening technique in U.S. airports;

2. Whether the TSA and respondents violated the Administrative Procedure Act, 5 U.S.C. § 553(e), in issuing the May 28, 2010 order refusing to process EPIC's April 21, 2010 5 U.S.C. § 553(e) petition ("the Second EPIC Petition");

3. Whether the DHS Chief Privacy Officer breached her statutory duty, 6 U.S.C. § 142, to prevent agency technology from eroding privacy protections by sanctioning the nationwide deployment of FBS devices in tandem with a systemized collection of airline passengers' personal information;

4. Whether the DHS Chief Privacy Officer failed to uphold her statutory duty, 6 U.S.C. § 142, to conduct adequate Privacy Impact Assessments when she neglected to identify and report numerous privacy risks in the design of airport body scanners;

5. Whether the Chief Privacy Officer failed to uphold the same statutory duty when she failed to conduct any formal assessment once the DHS entered a new, unpublished rule effectively subjecting all air travelers to FBS devices;

6. Whether the TSA and respondents violated the Fourth Amendment reasonableness requirement by routinely subjecting all air travelers to a uniquely invasive, suspicionless, and ultimately ineffective search of the most private areas of the human body;

7. Whether the TSA and respondents violated the Privacy Act by creating an indexed system of records containing air travelers' personally identifiable information without publishing a system of records notice in the Federal Register;

8. Whether the TSA and respondents' systematic rendering of detailed, three-dimensional images of air passengers' naked bodies violates the Religious Freedom Restoration Act by substantially burdening the free exercise of religion of those airline passengers who embrace sincerely held religious beliefs requiring the preservation of modesty;

9. Whether the TSA and respondents violated the Video Voyeurism Prevention Act by systematically capturing images described under the Act as constituting the "private area of the individual," including "the naked or undergarment clad genitals, pubic area, buttocks, [and] female breasts," and which would clearly offend any meaningfully definition of a reasonable expectation of privacy. 18 U.S.C. § 1801(b)(3).

STATUTES AND REGULATIONS

Statutes

STATEMENT OF FACTS

1) The Operation of Body Scanners

This case concerns the decision of the Respondent agency to deploy devices that are designed to capture and evaluate the contours of the human body that would not be visible to the naked eye as the primary screening technique in U.S. airports. Respondent has required that these devices have the ability to store, record, and transmit the images that are captured. Respondent has further required that these devices have "privacy filters" installed such that they may be disabled by Respondent. These devices are generally referred to as Whole Body Imaging ("WBI"), Full Body Scanners ("FBS"), or Automated Imaging Technology ("AIT").

Body scanners include both millimeter wave devices and backscatter x-ray. AR 11 at 3. Millimeter wave devices use non-ionizing radio frequency energy spectrum to generate a detailed, three dimensional image of the body based on the energy reflected from the body. *Id*. at 3. Backscatter technology uses a narrow x-ray beam that scans the surface of the body at a high speed. *Id*. Both types of devices capture in electronic storage a detailed image of the traveler that is then displayed on a remote monitor for analysis by a Transportation Security Official ("TSO"). *Id*. Filters designed to limit which parts of the human body may be

observed by the TSO may or may not be applied, depending on a decision of the Respondent.

To deploy the body scanners in U.S. airports, TSA has contracted with several companies, including American Science & Engineering (backscatter), L-3 Communications (millimeter wave) and Rapiscan Systems (backscatter). AR 8 at ___. In accordance with TSA's own requirements, these vendors design the body scanner machines to include Ethernet connectivity, USB access, and hard disk storage. AR 50 at ___; AR 51 at ___. These capabilities enable the capture, storage, and transfer of the images of the naked human body. The machines run an embedded version of Microsoft Windows XP (XPe), AR 125 at ___, that is prone to security vulnerabilities.

Travelers, privacy organizations, religious organizations, medical experts, and security experts have objected to the decision of Respondent to deploy body scanners in U.S. airports. AR 60 at 4-5; AR 65 at 1,8; AR 70 at 22; AR 95 at ___; AR 125 at ___. Travelers have expressed outrage at the invasiveness of the machines, the radiation exposure created by the machines, the lack of signage regarding the machines, and the absence of a meaningful alternative to the scans. AR 95 at ___. Experts in radiology and security have questioned the safety of the machines, and their effectiveness (especially regarding the detection of powdered explosives). AR 60 at 4-5, AR 65 at 1, 8; David Brenner, *Congressional*

Biomedical Research Caucus: Airport Screening: The Science and Risks of Backscatter Imaging, 2010, available at http://blip.tv/file/3379880; AR 70 at 22. Privacy advocates have taken issue with the machines' storage and transfer capabilities, the inadequacy of "privacy filters," and TSA's unwillingness to provide any meaningful alternative for travelers. AR 60 at 4-5; AR 125 at ___.

There are proposed alternatives to body scanners, including less intrusive passive millimeter wave technology and filters that indicate potential threats on an avatar instead of an actual passenger image. AR 70 at 18. A January 27, 2010 Government Accountability Office report states that TSA has ten passenger screening technologies in various phases of research, procurement, and development. *Id.*

2) Respondent's Deployment of Body Scanners in U.S. Airports

In 2007, TSA began pilot testing of full body scanners at checkpoints in three airports as an "optional method for screening selectees and other individuals requiring additional screening." AR 29; AR 44. Until February 2009, only forty body scanner units had been deployed in U.S. airports, and all for the purpose of secondary screening. AR 44; AR 29.

On January 2, 2008 the Agency published a Privacy Impact Assessment for the TSA Whole Body Imaging program that failed to identify numerous privacy risks to air travelers. AR 44 at ___. The Assessment did not examine or evaluate

the inherent privacy risks of devices specifically designed to include Ethernet connectivity, USB access, and hard disk storage. *Id.* Nor did the Assessment address the risk that TSA employees could bring recording devices, such as cell phones and digital cameras, into the remote viewing areas. *Id.*

During the spring of 2009, Respondent DHS made a determination that body scanners, which were previously only deployed for secondary screening in limited pilot projects, would in the future be deployed as the primary screening technique in U.S. airports. *See* AR 27; AR 28 ("Pilot Program Tests Millimeter Wave for Primary Passenger Screening"). Six of the forty body scanners in operation were re-deployed as primary screening units. AR 25. However, at no time during this period did the agency announce a rule or request public comment about the substantial change in agency practice.

On April 6, 2009, the New York Times reported that:

> In a shift, the Transportation Security Administration plans to replace the walk-through metal detectors at airport checkpoints with whole-body imaging machines — the kind that provide an image of the naked body.
>
> Initially, the machines were supposed to be used only on passengers who set off the metal detectors, to provide them with an option to the customary secondary physical pat-downs and inspections by electronic wand.

Joe Sharkey, "Whole Body Scans Past First Airport Test," The New York Times, Apr. 6, 2009, at B6.

On December 25, 2009, Umar Farouk Abdulmutallab boarded a United States-bound plane with a powered explosive hidden on his person that went undetected by screening procedures, even though he departed from an airport where body scanners were installed. AR 66. Following this incident, the DHS accelerated its plan to make body scanners the primary screening technique in U.S. airports. AR 64.

In January of 2010, the GAO released a report questioning if the body scanners would have been able to detect the powdered explosive weapon used in the December 25 attempted attack. AR 45. The GAO requested an independent survey to be conducted on this topic. *Id.* The results of this study are not available to the public.

As of May 7, 2010, Respondent has deployed fifty-eight body scanners in twenty-four airports across the country. AR 73 at 10. By the end of December of 2010, 492 units are scheduled to be deployed in the United States, and an additional 500 units in 2011. AR 75 at 7.

3) Absence of Meaningful Alternative to Body Scanner Search

As a matter of pattern, practice and policy, the TSA requires air travelers to submit to body scanner searches once they have entered the security zone in airports. AR 56 (numerous statements from air travelers, obtained by Petitioner EPIC under the Freedom of Information Act, describing this agency practice);

Schneier Decl. at ¶5 (“I watched a single TSA officer at the head of the line, telling some people to go through the Full Body Scanner, and others to go through the traditional magnetometer.”) Previously, the TSA used magnetometers (also called "metal detectors") to conduct mandatory, primary screening. Full body scans were optional, and were used only for secondary screening.

The TSA does not, in practice, offer air travelers an alternative to the body scanner search. AR 56 at ___. (Air traveler stated that “when he requested an alternative screening, the TSA screeners interrogated and laughed at him.”); *Id* at ___. ("I was asked/forced into this [body scanner] at BWI airport on 6/30/09”); *Id* at ___. (“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); *Id* at ___. (“the TSA guard sent my wife and I through the new X-Ray machine … A guard did not give us a choice.”); *Id* at ___. (“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.”)

Instead, the TSA claims to offer passengers a pat-down alternative, but many passengers are never informed of this option. Schneier Decl. at ¶¶7-9 (“I was not

verbally notified by any TSA official that the Full Body scan was optional … I did not observe any written notice or signage that indicated the Full Body scan was optional … I have no reason to believe that any traveler who went through security screening at Logan Airport at that time would have been told that the Full Body Scan was optional or that there was an alternative security screening procedure.”). There is also the growing sense, confirmed by the Respondent TSA’s statements, that these pat-downs have become particularly intrusive. Passengers perceive the pat-down to represent a retaliatory measure for those who do object to the body scanners. *Id* at ___. ("[I] decided to opt out [of a body scan]. My family and I were then subjected to a punitive pat-down search (they went over me three time) that would have been considered sexual assault in any other context").

4) Collection of Personally Identifiable Information

The TSA requires air travelers to disclose their full name, birth date, and gender when purchasing a ticket. The TSA requires air travelers to submit to searches at TSA airport security checkpoints and further requires that air travelers present a boarding pass and government-issued photo identification card at airport security checkpoints. AR 129; AR 130. The boarding pass displays air travelers’ full names, travel itineraries, and bar codes containing machine-readable versions of travelers’ personal information.

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. AR 19. 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. AR 128. The TSA is therefore able to associate a specific body scanner image with the full name, birth date, gender, and travel itinerary of the scanned traveler.

5) The EPIC Petitions to Require a Public Rulemaking and then to Suspend the Program

Following the recognition that the TSA had substantially changed its agency practice regarding the deployment of airport body scanners, on May 31, 2009, EPIC and thirty organizations petitioned DHS Secretary Janet Napolitano to suspend the body-scanner program and to conduct a 90-day formal public rulemaking. *See* AR 39. ("First EPIC Petition"). The First EPIC Petition urged the DHS to consider public input and to fully evaluate all privacy, security, and health risks the devices pose, and to investigate less invasive means capable of the same security outcomes. *Id*.

On June 19, 2009, the Acting Administrator of TSA, Gale D. Rossides, sent a letter to EPIC on behalf of Secretary Napolitano. *Id.* The letter assured all signees of the petition that the agency was in a constant search for ways to improve its outreach and education. *Id.* The letter did not address the request for a formal

rulemaking set out in the First EPIC Petition, and the agency did not initiate a rulemaking. *Id.* To date, DHS has failed to act on the First EPIC Petition.

On January 11, 2010, DHS responded to a Freedom of Information Act request submitted by Petitioner EPIC, disclosing the technical specifications and vendor contacts for the agency's body scanners. *See* AR 50. The documents obtained by Petitioner EPIC revealed the machines' capability to store, record, and transfer images of naked air travelers. *See id.* Throughout March and April of 2010, DHS released to Petitioner EPIC additional documents, including hundreds of traveler complaints regarding the body scanner machines. *See* AR 56. The complaints described a variety of problems with the machines, as well as passenger objections to the invasive nature of the machines and complaints about improper signage and a lack of transparency regarding the pat-down alternative. *See id.*

On April 21, 2010, EPIC and thirty privacy, consumer, and civil rights organizations sent a second petition to DHS Secretary Napolitano, this time also addressing DHS Chief Privacy Office Mary Ellen Callahan. AR 125. ("Second EPIC Petition"). The Second EPIC Petition was signed by several religious organizations, including the Asian American Legal Defense and Education Fund ("AALDEF"), the Council on American Islamic Relations ("CAIR"), and the Muslim Legal Fund of America ("MLFA"). *Id.* The Second EPIC Petition charged that the pending deployment of body scanners in U.S. airports "violates the U.S.

Constitution, the Religious Freedom Restoration Act, the Privacy Act of 1974, and the Administrative Procedure Act." *Id.* The Second EPIC Petition further noted that "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 airline bombing." *Id.*

EPIC documented the agency's silence regarding the First EPIC Petition, the agency's announcement of one thousand additional body scanner devices in airports across the country, and the agency's new, unpublished rule mandating the use of FBS devices in primary screening. *See id*. After explaining how this new agency procedure violated the constitutional and statutory rights of millions of Americans, EPIC and the organizations petitioned the agency to "immediately suspend purchase and deployment of full body scanners to American airports." EPIC and the organizations requested that the DHS and TSA "cease operation of already deployed Full Body Scanners as primary screening." To date, DHS has failed to process EPIC's second petition.

On May 28, 2010, the Chief Counsel of the TSA, Francine J. Kerner, sent a letter on behalf of Secretary Napolitano and Chief Privacy Officer Mary Ellen Callahan. AR 125. The letter asserted that the TSA is not legally required to initiate an APA rulemaking "each time" it implements passenger screening procedures. *Id*. at ___. However, the letter did not acknowledge that the agency

had decided on its own authority, and without a public rulemaking, to pursue the airport body-scanner program as the primary screening technique. The letter further stated that "*use of AIT screening is optional for all passengers*" (emphasis in original), but failed to note the many complaints from travelers who are not provided an option. *Id*. Moreover, in the discussion of the RFRA concerns, the TSA simply asserted a compelling interest in the body scanner screening procedure that would appear to nullify not only the concerns of those travelers with sincere religious objections but any traveler who might choose to object to the invasive procedure. *Id.* at __.

6) Opposition to Full Body Scanners Expressed by Members of Congress

Congress has made clear its dissatisfaction with the attempts by Respondent to extend the reach of the airport body scanner program. In June 2009, following the Respondent's unilateral decision to make body scanners the primary screening technique, the Congress approved a bill that would limit the use of body scanners in U.S. airports. H.R. 2200, 111th Cong., *as amended by* H. Amend. 172 (1st Sess. 2009). Congressman Jason Chaffetz (R-UT) sponsored the bill that would prohibit the use of the devices as the sole or primary method of screening aircraft passengers; require that passengers be provided information on the operation of such technology and offered a pat-down search in lieu of such screening; and

prohibit the storage of an image of a passenger after a boarding determination is made. *Id.* The Senate has yet to take up the measure.

Senators and Representatives, in many public communications with Respondents, have also made known their concerns about the program. On January 20, 2010, Senators Coburn (R-OK), and Akaka (D-HI) of the Senate Committee on Homeland Security and Government Affairs questioned DHS Secretary Janet Napolitano about the body scanners' inability to detect small amounts of explosives. AR 65 at 1. They also inquired about the lack of operational testing before body scanners are deployed and the potential risk relating to "unhealthy levels of radiation." *Id*. at 3-8.

On February 24, 2010, the Chairman of the House Committee on Homeland Security, Representative Bennie G. Thompson, wrote on the Committee's behalf to inquire about the "apparent contradiction" between the TSA's representations to the public and the technical capabilities which allow its body scanner devices to "erode individual privacy protections." AR 81 at 4. Chairman Thompson demanded to know the TSA's reasoning for requiring the body scanner devices to store, print, record, and export images, and the circumstances under which TSA employees can use these capabilities in airport settings. *Id*. The Chairman also asked if the TSA requested the Chief Privacy Officer to amend of update previous Privacy Impact Assessments. *Id*.

On August 6, 2010, three U.S. Senators objected to the DHS's expansion of the airport body scanner program. In a letter to DHS Secretary Janet Napolitano, Senators Collins (R-ME), Burr (R-NC), and Coburn (R-OK) asked "why the Department continues to purchase this technology when legitimate concerns about its safety appear to remain unanswered." Letter from Senators Collins, Burr, Coburn to DHS Secretary Janet Napolitano (Aug. 6, 2010), *available at* http://www.epic.org/redirect/090110senatorsletter.html. The Senators noted that "the issue of radiation associated with the backscatter x-ray AIT machines has not been adequately addressed by TSA." They urged the agency's Chief Medical Officer, working with independent experts, to conduct a review of the health effects on travelers and airport personnel. *Id.*

On August 19, 2010, the Chairman and Ranking Member of the Homeland Security Committee, along with four other Senators, sent a letter to the head of the US Marshals Service to ask why the federal agency stored more than 35,000 images from whole body imaging scans taken at the Orlando federal courthouse. Letter from Senators Leiberman, Collins, Akaka, Carper, Chambliss, Isakson to John F. Clark, USMS *(*Aug. 19, 2010), *available at* http://www.epic.org/Senators_Letter_US%Marshals_8-19-10.pdf. The letter followed a Freedom of Information Act lawsuit, filed by EPIC, in which the Marshals Service was forced to disclose the fact that it had stored body scanner

images. In their letter, the senators urged the agency to examine and adopt privacy protocols, including a prohibition of the storage and transfer of body scanner images. *Id.*

7) Petitioner's Motion for Emergency Stay

Following Respondent's failure to act on either the First EPIC Petition or the Second EPIC Petition, as well as the concerns expressed by Members of Congress, and anticipating the Respondent's intent to accelerate the deployment of body scanners in U.S. airports, Petitioner filed a Motion for Emergency Stay of the Agency's Rule on July 2, 2010.

SUMMARY OF ARGUMENT

Respondent agency has initiated the most sweeping, the most invasive, and the most unaccountable suspicionless search of American travelers in history. Respondent has subjected millions of air travelers to suspicionless searches that target the most intimate areas of the human body. It has deployed devices, of its own design, that have the ability to store, record, and transmit these images of the naked human body. And it has done so in disregard of federal statutes and Constitutional safeguards that are intended to protect the privacy and religious rights of individuals and to ensure accountability in agency decision-making. It has even disregarded a federal privacy law that explicitly prohibits the capture of naked images by federal officials where there is a reasonable expectation of privacy.

Petitioner EPIC has carefully, and with due regard to legitimate security concerns in the nation's airports, compiled an extensive record that includes the technical specifications and contracts for the body scanner devices. Petitioner EPIC has also obtained hundreds of complaints from air travelers that detail the public objections to Respondent's program as well as the specific concern that air travelers are not told about an alternative to the body scanner, a central claim on which Respondent relies. These documents were all obtained by EPIC from Respondent prior to the initiation of this litigation through a series of Freedom of

Information Act lawsuit. There is no dispute as to the authenticity of the documents upon which Petitioners rely.

In the spring of 2009, Petitioner EPIC became aware that Respondent intended to dramatically transform airport screening procedures in the United States and make body scanners the primary screening technique in all airports. Until this time, the body scanners were deployed as part of a pilot program with the explicit assurance that they would only be used for secondary screening and also that, even in the case of secondary screening, a meaningful alternative would be available.

In recognition of the substantial change in agency practice that would affect the interests of millions of air travelers in the United States, Petitioner EPIC and a coalition of organizations urged the Secretary of the Department of Homeland Security to undertake a public rulemaking so that there might be an opportunity for the public to express its views on the agency rule and for the agency to consider less intrusive alternatives.

Respondents failed to respond to Petitioner's request, and when the agency subsequently made known its intent, early in 2010 following the trouser bomb incident, Petitioner and a coalition of thirty civil rights, civil liberties organizations, including many religious organizations, urged the Secretary to

suspend the program. Again, Respondent failed to acknowledge the petition, 5 U.S.C. 553(e), of Respondent, and continued the deployment of the devices.

In the arguments below, Petitioners set out the various statutory and Constitutional claims that are implicated by the agency's conduct. However, it is not Petitioner's position that these devices may never be deployed or that the security concerns in the nation's airports are not substantial. It is simply that in developing airport security standards, Respondent must comply with relevant law, and it must not be permitted to engage in such a fundamental change in agency practice without providing the public the opportunity to express its views and taking into account those views in its final rule, as the Administrative Procedure Act requires.

STANDING

Petitioner EPIC has two distinct standing claims in this matter. The first arises from Respondent's failure to act on EPIC's petition, submitted pursuant to the Administrative Procedure Act, 5 U.S.C. § 553(e). The second arises from Article III of the Constitution which permits and organization to bring a claim on behalf of its members.

Under the Administrative Procedure Act, 5 U.S.C. § 551, and the provisions that govern judicial review of Aviation Programs, 49 U.S.C. § 46110, Petitioner EPIC is entitled to review of a determination by Respondent regarding the two petitions it submitted concerning the deployment of airport body scanners in the United States.

EPIC also has standing under Article III of the Constitution of the United States. An association has standing to sue on behalf of its members if (1) at least one of its members would have individual standing to sue in his or her own right, (2) the interests the association seeks are germane to its purpose, and (3) neither the claim asserted nor the relief requested requires that an individual member of the association participate in the lawsuit. *Sierra Club et al. v. EPA et al.*, 292 F.3d 895 at 896-97 (D.C. Cir. 2002) (citing *Hunt v. Washington State Apple Advertising Comm'n*, 432 U.S. 333 (1977)). Declarations from members of an organization are sufficient to establish standing for judicial review of administrative action.

"Because [the organizations'] claims and requested relief are germane to their organizational purposes and do not require any individual member to participate in the lawsuit, the organizations have standing to sue on behalf of those members." *Theodore Roosevelt Conservation Partnership v. Salazar*, 616 F.3d 497, 507 (D.C. Cir. 2010).

Regarding the first element, Respondent should readily concede that members of the association will be subject to the airport body scanner program, as any person traveling by air in the United States is subject to the airport screening procedures established by the TSA.

The second element of EPIC's standing is manifestly apparent. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has a specific interest in Respondent's body scanner rule, as made clear in EPIC's two petitions to Respondent DHS, AR 39; AR 125, in addition to a long-standing interest in DHS and TSA practices implicating the privacy rights of travelers.

EPIC routinely comments on agency rulemaking regarding air traveler privacy. *See, e.g.,* Biometrics Guidance Notice, 70 Fed. Reg. 10667, Docket No. TSA-2005-20485 (Mar. 4, 2005) (EPIC urged the TSA to conduct a Privacy Impact Assessment, to enforce Privacy Act standards, and to incorporate privacy safeguards in connection with access control systems in the nation's airports); In

the Matter of Privacy Act System of Records Notice, Registered Traveler Operations Files, 69 Fed. Reg. 30948, Docket No. TSA-2004-17982 (June 1, 2004) (EPIC urged the TSA not to approve the final phase of the Registered Traveler program until the agency and revised its information collection and maintenance practices to comply fully with the intent of the Privacy Act.)

EPIC has also testified before Congress on air travel privacy several times. *See* Testimony of Marc Rotenberg, *An Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe?* Before the House Comm. on Homeland Security, Subcomm. on Trans. Sec. and Innovation Protection , 111th Cong, 2nd Sess., ___ (Mar. 17, 2010); Testimony of Marc Rotenberg, EPIC President, *Passport Files: Privacy Protection Needed For All Americans*, Before the Senate, Comm. on the Judiciary, 110th Cong., 2nd Sess., ___ (July 10, 2008); and, Testimony of Marc Rotenberg, EPIC President, *The Future of Registered Traveler,* Before the House Subcomm. on Economic Sec., Infrastructure Protection, and Cybersecurity, Committee on Homeland Security, 109th Cong., 1st Sess., ___ (Nov. 3, 2005)

Regarding the third element set out in *Sierra Club*, it is not necessary for individual members to participate in the lawsuit to assert these claims or to request relief, but members of the association have chosen to do so.

Petitioners Bruce Schneier and Chip Pitts, who are Advisory Board Members of EPIC, also have standing in their individual capacity. Mr. Schneier filed a formal declaration with this Court stating that he was "instructed by [a] TSA officer to go through a Full Body Scanner device, operated by the TSA." Schneier Decl. at 2. He further stated that he "did not observe any written notice or signage that indicated the Full Body scan was optional or that there was an alternative security screening procedure," and that he "was not verbally notified by any TSA official that the Full Body scan was optional or that there was an alternative security screening procedure." *Id*.

Mr. Pitts is the immediate past-President of the Bill of Rights Defense Committee and a Lecturer at Stanford Law School. He travels frequently, has experienced the Full Body Scanner devices operated by TSA and as is the case for most air travelers as Respondents would concede, can reasonably expect to be subject to Respondent's airport body scanner program again in the near future.

Petitioner Al-Khalili has standing to sue in her individual capacity. Nadhira Al-Khalili, Esq. is Legal Counsel for Council on American-Islamic Relations ("CAIR") in Washington, DC and routinely travels by for both personal and business reasons. She can reasonably expect to be subject to the body scanner program. Al-Khalili decl. at 2. Moreover, her organization CAIR signed the Second EPIC Petition which sets out the various claims alleged in this matter.

Mr. Schneier, Mr. Pitts, and Ms. Al-Khalilis' standing as petitioners depends on (1) injury-in-fact, (2) causation, and (3) redressability." *Sierra Club* at 897, quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992) (internal citations omitted).

The injury in fact to Petitioners Schneier, Pitts, and Al-Khalili are the violations of federal law, cited by Petitioner EPIC in the petition to Respondent. These include the failure to undertake a System of Records Notice, as required by the Privacy Act. The collection of naked images of the human body is prohibited by the Video Voyeurism Prevention Act. Most significantly, Petitioners Schneier, Pitts, and Al-Khalil, believe that the invasive, suspicionless search enabled by Respondent's airport body scanner Rule is unreasonable and therefore a violation of their Fourth Amendment rights.

Petitioner Al-Khalili has the additional claim that Respondent's body scanner program substantially burdens her free exercise of religion and is therefore a violation of the Religious Freedom Restoration Act.

There is no dispute as to causation – the body scanners are deployed by Respondent, pursuant to a Rule adopted by Respondent, in a facility controlled by respondent. Nor is there any dispute as to redressability, as Respondent could revise its airport screening programs to comply with federal laws.

If the body scanning program is not halted, or, in the alternative, if DHS is not, at minimum, required to respond to EPIC's request for a 90-day rulemaking, then the injuries complained of will continue into the future.

ARGUMENT

I. The TSA's Full Body Scanner Program Violates the Administrative Procedure Act

A. The TSA Improperly Processed EPIC's Section 553(e) Petitions

"Each agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule." 5 U.S.C. § 553(e). "The right to petition for rulemaking entitles the petitioning party to a response on the merits of the [Section 553(e)] petition." *Fund for Animals v. Babbitt*, 903 F. Supp. 96, 115-16 (D.D.C. 1995) (citing *American Horse Protection Ass'n, Inc. v. Lyng*, 812 F.2d 1, 4 (D.C. Cir. 1987)). "Agencies denying rulemaking provisions must explain their actions." *Fund for Animals*, 903 F. Supp. at 115. *Families for Freedom v. Napolitano*, 628 F. Supp. 2d 535, 540 (S.D.N.Y. 2009) (". . . it is clear that DHS is required to at least definitively respond to plaintiff's petition – that is, to either deny or grant the petition.").

"Under the APA, a federal agency is obligated to conclude a matter presented to it within a reasonable time." *In re American Rivers & Idaho Rivers United*, 372 F.3d 413, 418 (D.C. Cir. 2004); 5 U.S.C. § 555(b). "A reviewing court

may 'compel agency action unlawfully withheld or unreasonably delayed.'" *Id*. (quoting 5 U.S.C. § 706(1)). "There is no *per se* rule as to how long is too long to wait for agency action, but a reasonable time for agency action is typically counted in weeks or months, not years. *Id*. at 419 (internal citation and quotations omitted).

EPIC filed the First EPIC Petition on May 31, 2009, urging the DHS to undertake "a 90-day formal public rulemaking process to receive public input on the agency's use of [full body scanners]." Exhibit 1. The First EPIC Petition's language unambiguously "petitions for the issuance" of an agency rule. The DHS is required to, at a minimum, grant or deny EPIC's petition, and do so within "a reasonable time." The DHS has failed to act on the First EPIC Petition through the date of this filing, more than one year later. *See* Exhibit 2 (discussing, but failing to act on, the First EPIC Petition). The DHS's failure to act has created an unreasonable delay that exceeds mere "weeks or months." Indeed, the DHS was recently ordered to process an unreasonably delayed APA petition; the agency had delayed action for more than one year. *Families for Freedom*, 628 F. Supp. 2d at 535. The DHS's one-year delay in processing the First EPIC Petition is unreasonable as a matter of law.

On April 21, 2010, Petitioner EPIC filed 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." Exhibit 3. On May 28, 2010, the TSA

issued an order refusing to process the Second EPIC Petition. Exhibit 4 at n.1. The TSA's order plainly violates the APA. The TSA effectively ignored a document explicitly marked as a "petition" filed "pursuant to 5 U.S.C. § 553(e)." Well-established law "entitles [Petitioners] to a response on the merits." *Fund for Animals*, 903 F. Supp. at 115-16.

B. The DHS Privacy Office Failed to Comply With its Statutory Mandate to Protect Travelers' Privacy

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." 6 U.S.C. § 142(1) (2009). The DHS Chief Privacy Officer also has a statutory obligation to ensure the agency's compliance with the Privacy Act, including the duty 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." 6 U.S.C. § 142(2)-(4).

The DHS Chief Privacy Office prepared an inadequate Privacy Impact Assessment of the TSA's FBS test program which failed to identify numerous privacy risks to air travelers. AR 25. 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.

II. Respondent's Body Scanner Program Violates the Fourth Amendment

Petitioners do not dispute that the TSA has broad authority to conduct searches at airport security checkpoints. *See United States v. Aukai*, 497 F.3d 955, 960 (9th Cir. 2007)("Airport screening searches are constitutionally reasonable administrative searches").

However, the TSA's authority is not boundless.

> The scope of such searches is not limitless. A particular airport security screening search is constitutionally reasonable provided that it is no more extensive nor 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.

Aukai, 497 F.3d at 962 (*citing U.S. v. Davis*, 482 F.2d 893, 913 (9th Cir. 1973)) (emphasis added). Even when administrative security interests are "legitimate and substantial," the interests "cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved." *Shelton v. Tucker*, 364 U.S. 479, 488 (1960). Fourth Amendment safeguards "dictate a critical examination of each element of the airport security program." *Davis*, 482 F.2d at 913.

Courts require that airport security searches be "minimally intrusive," "well-tailored to protect personal privacy," and "neither more extensive nor more intensive than necessary under the circumstances to rule out the presence of weapons or explosives." *U.S. v. Hartwell*, 436 F.3d 174, 180 (3d Cir. 2006); *Aukai*,

497 F.3d at 962. Searches are reasonable if they "escalat[e] in invasiveness only after a lower level of screening disclose[s] a reason to conduct a more probing search." *Hartwell*, 436 F.3d at 180.

The TSA's full body scanner program fails to meet these standards. The TSA subjects all air travelers to the most extensive, invasive search available at the outset. The TSA searches are also far more invasive than necessary to detect weapons. Alternative technologies, including passive millimeter wave scanners and automated threat detection, detect weapons with a less invasive search.

Far from the "minimally intrusive" searches upheld in *Aukai* and *Hartwell*, the TSA rule requires individuals to submit to a digital strip search that is maximally intrusive. Further, unlike the escalating searches at issue in *Aukai* and *Hartwell*, the TSA body scanner rule subjects all travelers to the most invasive search available as primary screening, without any escalation. Aukai and Hartwell were first scanned by walk-through magnetometers. *Aukai*, 497 F.3d at 962; *Hartwell*, 436 F.3d at 180. Magnetometers detect metal, but, unlike body scanners, produce no naked image of the traveler and retain no record. After Aukai and Hartwell set off alarms on walk-through magnetometers, they were screened with "wands" – hand-held magnetometers. *Id*. Wands are also less invasive than body scanners – wands produce no naked image of the traveler and retain no record. After Aukai and Hartwell set off alarms on the wands, security agents asked them

to empty their pockets. *Id*. This procedure is also less invasive than body scanners. Only after this procedure revealed additional evidence of contraband were Aukai and Hartwell subjected to the maximally invasive search.

IV. Respondent's Body Scanner Program Violates the Privacy Act

As described above, the TSA's Full Body Scanner Program creates a system of records containing air travelers' personally identifiable information. The system 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. Yet, the TSA failed to publish a "system of records notice" in the Federal Register, and otherwise failed to comply with its Privacy Act obligations. 5 U.S.C. § 552a(e)(4).

V. Respondent's Body Scanner Program Violates the Religious Freedom Restoration Act

The Religious Freedom Restoration Act ("RFRA") bars the government from placing a substantial burden on a person's exercise of religion even if the burden arises from a rule of general applicability, unless the government demonstrates a compelling governmental interest, and uses the least restrictive means of furthering that interest. *Holy Land Found. for Relief & Dev. v. Ashcroft,* 333 F.3d 156 (D.C. Cir. 2003), *see also* 42 U.S.C. § 2000bb-1(a), (b). The use of FBS at the airport violates the RFRA because the capture and transmission of

naked images of individuals offends the sincerely held beliefs of Muslims and other religious groups. Muslims believe in maintaining modesty and covering their bodies. FBS enables the capture and viewing of naked human images that violates this belief and denies observant Muslims the opportunity to travel by plane in the United States as others are able to do. *See, e.g.*, Jane Perlez, "Upset by U.S. Security, Pakistanis Return as Heroes," N.Y, Times, Mar. 9, 2010 at A4.

A. The TSA is Substantially Burdening Travelers' Exercise of Religion

An impermissible burden exists when government action puts "substantial pressure on an adherent to modify his behavior and to violate his beliefs…" or "perform acts undeniably at odds with fundamental tenets of [his] religious beliefs." *Kaemmerling v. Lappin*, 553 F.3d 669, 677 (D.C. Cir. 2008) (*quoting Thomas v. Review Bd.*, 450 U.S. 707, 718, 101 S. Ct. 1425 (1981); *Wisconsin v. Yoder*, 406 U.S. 205, 218 (1972).

"Exercise of religion" includes "any exercise of religion, whether or not compelled by, or central to, a system of religious belief." *Mahoney v. District of Columbia,* 662 F. Supp. 2d 74, 96 (D.D.C. 2009); 42 U.S.C. § 2000bb-2(4). What matters is not the centrality of the particular activity to the religion but rather whether the adherent's sincere religious exercise is substantially burdened. *Id*.

Here, the government substantially burdens the devout air travelers' religious exercise. Forcing a Muslim individual to undergo FBS conflicts with the

maintenance and preservation of modesty, beliefs central to the tenets of Islam, and is therefore a substantial burden. *See, e.g.,* AR 87 (describing a Muslim woman who refused a body scan at an airport). Muslims are encouraged to cover most of their body in an effort to maintain modesty, a central belief in the faith, especially in front of individuals of the opposite gender. The Fiqh Council of North America, which addresses religious issues of Muslims living in America, objected to the use of FBS, stating that the machines are "against the teachings of Islam, natural law and all religions and cultures that stand for decency and modesty." AR 125, at ___. "It is a violation of clear Islamic teachings that men or women be seen naked by other men and women. Islam highly emphasizes 'haya' (modesty) and considers it part of faith." *Id*.

Many travelers have been forced to go through FBS machines at various airports prior to boarding flights. Many travelers were not informed that their bodies would be exposed nor that their images would be viewed by individuals of the opposite gender. Religious travelers are offered the Hobson's choice of either violating their beliefs or not traveling. This "choice" is similar to that presented in *Sherbert v. Verner,* where the Court held that the government unlawfully burdened the plaintiff because she could "choose between following the precepts of her religion and forfeiting benefits, on the one hand, and abandoning one of the precepts of her religion in order to accept work, on the other hand." *Sherbert v.*

Verner, 374 U.S. 398, 404 (1963). In this way, TSA forces travelers to "perform acts undeniably at odds with fundamental tenets of their religious beliefs." *Wisconsin,* 406 U.S. at 218.

B. The TSA's Use of Body Scanner Technology is not the Least Restrictive Means

A statute or regulation is the least restrictive means if no alternative forms of regulation would accomplish the compelling interest without infringing religious exercise rights. *Kaemmerling v. Lappin*, 553 F.3d 669, 684 (D.C. Cir. 2008). In considering whether the practice is the least restrictive means possible, the government must consider and evaluate the efficacy of other less restrictive options. *Sample v. Lappin,* 424 F.Supp 2d. 187, 195 (D.D.C. 2006).

Aviation security is a compelling government interest. But full body scanners are not the least restrictive means of advancing that interest. The TSA's scanners are deeply flawed. The TSA refused to conduct a cost-benefit analysis, despite repeated calls for such an analysis by the Office of Inspector General.

There are other effective means for screening passengers that would be less intrusive and would not substantially burden the religious practice of Muslims and other religious groups. The TSA concedes the possibility of other effective methods – on TSA's website, the combination of a metal detector and pat-down search is discussed as a possible alternative to FBS technology. TSA, *TSA: Imaging Technology.* Some other examples of less intrusive methods are: passive

millimeter wave scanners and automated threat detection. These methods would allow for effective detection of threats without subjecting travelers to an invasive search that violates one of their most basic religious tenets.

VI. Respondent's Program Violates the Video Voyeurism Prevention Act

The Video Voyeurism Prevention Act of 2004 specifically prohibits the intentional "capture [of] an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, . . ." 18 U.S.C. §1801 (2010). The "private area of the individual" is defined as "the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual." 18 U.S.C. §1801(b)(3) These "private areas" are routinely captured by Full Body Scanners as numerous images demonstrate. *See, e.g.*, Exhibit 1.

The Act permits an exception for "any lawful law enforcement, correctional, or intelligence activity," 18 U.S.C. §1801(c), but because a body scanner search is unlawful under the Fourth Amendment, as set out above, this exception would not apply. Significantly, the Act seeks to protect individuals whose private images may be captured in public places. *See* H.R. Rep. No. 108-504, at 3 (2004). The Act explicitly defines "circumstances in which the individual has a reasonable expectation of privacy" as those "in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of

whether that person is in a public or private place." 18 U.S.C. §1801(b)(5)(B). Exhibit 1 makes clear that this standard is met.

CONCLUSION

Petitioners do not object to the use of Full Body Scanners in all circumstances. In fact, body scanners may be a preferred technique for secondary screening where circumstances require a more careful examination of particular passengers. Scanners may also be preferable for passengers with prosthetics and other devices that routinely trigger magnometers.

Petitioners object to Respondents' decision to make Full Body Scanners the primary means of screening in US airports. That decision disregarded the Fourth Amendment, as well as federal laws that ensure agency accountability and help safeguard privacy and religious freedom. Respondents have broad authority to undertake screening of travelers at airports in the United States, but such authority is not unbounded. Petitioners respectfully urge this court to enjoin the Agency Rule until DHS undertakes a formal 90-Day rulemaking procedure, and to provide for such further relief as this court determines.

Respectfully submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW

Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier

/s/ Nadhira Al-Khalili
NADHIRA AL-KHALILI
453 New Jersey Ave., South East
Washington, DC 20003
(202) 488-8787
Pro se Petitioner

Dated: November 1, 2010

TYPE/VOLUME CERTIFICATE OF COMPLIANCE WITH RULE 32(A)

I hereby certify that the foregoing brief complies with the typeface requirements of F.R.A.P. 32(a)(5) and the type-style requirements of Rule 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Rule 32(a)(7)(B)(iii).

/s/ Marc Rotenberg
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 1st day of November, 2010, he caused the foregoing brief to be served by ECF and two hard copies by first-class mail, postage prepaid, on the following:

John S. Koppel
Douglas Letter
U.S. Department of Justice, Appellate Staff, Civil Division
950 Pennsylvania Avenue, N.W.
Room 7264
Washington, D.C. 20530
P: (202) 514-3311

/s/ Marc Rotenberg
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioners Electronic Privacy Information Center, Chip Pitts, and Bruce Schneier