No. 10-1157

SCHEDULED FOR ORAL ARGUMENT ON MARCH 10, 2011

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.

REPLY 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 (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009

* Ms. McCall is admitted to practice in Pennsylvania. Admission to the District of Columbia bar pending. EPIC Fellows Conor Kennedy and Nichole Rustin-Paschal participated in the preparation of this brief.

(202) 483-1140
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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Authorities

STATEMENT OF THE CASE

Respondents state at the outset that "Since September 11, terrorist threats to air travel have continued to rise" and that "threats to aviation security constantly change and become more sophisticated." Pet. Br. at 3. But neither statement, on close inspection, is true. The events on September 11, 2001 were horrific and resulted in the deaths of almost 3,000 people. Since that day, not a single person has died or been injured as a result of a terrorist threat to commercial air travel in the United States. Moreover, prior to September 11, 2001 aircraft were hijacked at a rate of approximately one dozen per year and passengers were killed by those who seized control of planes.

The second statement is equally false. The attack on September 11 required the coordinated efforts of twenty trained individuals, supported by an elaborate network, operating over a two-year period, leading to the commandeering of four commercial aircraft in US airspace. *See generally* National Commission on Terrorist Acts Upon the United States, *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. The September 11 attack was absolutely unprecedented and to describe recent efforts by a few individuals to conceal small amounts of explosive material in shoes and underwear as "more sophisticated" is to render words without meaning.

Any reasonable characterization of aviation security at this time would begin by noting that air travel is far safer today than it was on September 11, 2001, which begs the question, now before this Court, why air travelers in the United States should be subjected to the most invasive, ineffective, suspicionless search ever conceived.

STATEMENT OF THE FACTS

A. Statutory and Regulatory Authority

Congress made clear that the TSA's deployment of advanced airport checkpoint systems would be part of a "pilot program" under which it would "deploy and test" the technology. 49 U.S.C. § 44925 note. Congress never gave the agency authority to mandate these new screening procedures. The significance of these terms becomes clear from the 2008 Senate Report, which set out the conditions for "operational deployment" of the technology:

> The final decision on the operational deployment of a technology should be based on the performance, reliability, cost, and maintainability of the machines. These technologies should only be deployed if appropriate privacy filters have been established.

S. Rep. No. 11-0396, at 60 (2008). The Committee contemplated that there would be a "final decision" prior to "operational deployment" and that there would be "appropriate privacy filters" prior to any deployment.

As to the invasiveness of the search, the images obtained and viewed are neither "fuzzy photo negatives" or "chalk etchings." Resp't Br. at 10. The devices capture detailed images of human genitalia, breasts, the buttocks, and other intimate parts of the human body. AR 051.011-051.012. The devices have zoom capability so that the TSO can examine specific areas of the human body in greater detail. Even the images that the TSA displays in airports are not of fuzzy photo negatives or chalk etchings. AR 047.023.

1. Opting Out

TSA maintains that it "communicates and provides a meaningful alternative to AIT screening," Resp't Br. at 11, but among the most frequent traveler objections to the program is the fact that travelers are not told of an alternative. Pet. Br. at 11; Schneier Decl. at ¶¶7-9. Moreover, when travelers select the pat-down, they often describe it as "coercive" or "retaliatory." Pet. Br. at 10-12. The fact that the majority of passengers go through the body scanner does not prove that they "selected" it.

2. Privacy Safeguards

Respondents' characterization of the "privacy safeguards" is not accurate and also raises new questions. Respondent DHS previously maintained that individuals could not be identified because facial images were blurred. DHS

Privacy Office 2010 Annual Report at 55. Now respondents state "images do not show sufficient detail for personal identification." Resp't Br. at 12. Elsewhere, respondents contend that the devices produced "chalk images" and "fuzzy negatives." *Id.* at 10. Regardless of whether "facial blurring," "chalk images," or "fuzzy negatives," conceal some features from the operator viewing the image – respondents are inconsistent at best as to which technique is deployed – none of the characterizations accurately describe the images in the record. AR at 047.023. The device is, in fact, designed to capture and record an unfiltered image of the naked human body in extraordinary detail. AR at 051.011-051.012. This point is critical to understand the actual privacy risk. Every step that the TSA claims to take to obscure the image of the naked human body can be easily undone, much as a lens filter can be placed on a camera lens and then removed from a camera lens, or a digital camera may allow the owner to view an image in black and white, with a sepia tone, or with colors inverted. These are merely photo processing techniques that do not obviate the need for the collection of the actual, raw image in the first instance. See AR at 051.011-051.012.

Respondents further maintain that with the TSO "located remotely from the individual being screened . . . within a walled and locked room" there "is no possibility that the transportation security officer will be able to connect the image on the screen to any individual being scanned." Resp't Br. at 12. However, the

TSO observing the images on the display screen and the TSO observing the passenger at the security checkpoint are communicating in real time with wireless headsets, which respondent elsewhere acknowledges. Resp't Br. at 49. Here the TSO is described as if in an isolation chamber, which is not accurate.

Second, respondents maintain that the devices deployed in airports "cannot store images." Resp't Br. at 12. This is not a truthful statement. It is similar to stating that a laptop computer previously configured to print to an Epson printer "cannot" print to a Cannon printer. One need only install the software drivers to enable the obvious functionality of the device. The TSA is also not forthcoming about how easily this change could be made. Resp't Br. at 12. Some TSA officials, as indicated in the technical specifications, have the access control to enable the storage, recording, and export of unfiltered images in the airports. AR at 051.011-051.012, 051.061.The change would be even easier than reconfiguring a printer for a laptop since all of the functionality is already contained in the device.

Respondent elsewhere mischaracterizes the functionality of the device and describes "a factory setting, which cannot be changed by the operator, prevents the image from being stored." Rep. Br. at 19. The statement is not true insofar as (1) the setting is not under the control of the "factory," but the agency itself, and (2) the "operator" could include a TSA official with the authority and ability to enable the storage and recording of images. Respondent tries the gambit again at 50,

stating, "the technology's capability for storing images is disabled by the manufacturer prior to being deployed and cannot be activated by the transportation security officers on site." First, the technology's "capability" for storing images can never be disabled as the devices are designed to store images and "capability" means literally "having the ability" to do something, whether or not it is in fact done. Second, a TSA official with the appropriate password can enable the storing and recording of images in airports. AR 050.011-.012, .061.

3. Safety Evaluation

As to the safety evaluation, Respondents cite a series of studies, none of which were undertaken in an operational environment. Resp't Br. at 13-14. Moreover, the decision of the agency not to conduct a formal rulemaking meant that the agency could disregard contradictory evidence as well as the possible risks resulting from the malfunctioning of the devices.[1]

[1] *See, e.g.,* Susan Stellin, "Are Scanners Worth the Risk?" N.Y. Times, Sept. 7, 2010, at TR3 ("Peter Rez, a physics professor at Arizona State University, has been pushing for more data to be shared so that academics can do their own analysis. 'The scary thing to me is not what happens in normal operations, but what happens if the machine fails,' Professor Rez said. 'Mechanical things break down, frequently.' . . . 'It's premature to put a whole population through this thing, not without much more due diligence and much more independent testing,' said John Sedat, a biochemistry professor at the University of California, San Francisco, who, along with several colleagues, sent a letter to the Obama administration calling for independent evaluations of the X-ray scanners.")

C. Efficacy of FBS

Respondents do not state that FBS has actually detected a threat to aviation safety – the presence of a concealed "substance," such as contraband, does not constitute a threat – nor do they demonstrate that the devices are, in practice, more effective than other airport screening procedures. Moreover, respondents have not established that the devices satisfy the "performance" or "reliability" requirements set out by the Senate Appropriation Committee, *supra*. Respondents are remarkably silent on the question of whether this technology is designed to detect, or could in practice detect, the powdered explosive of the type involved in the trouser bomber incident. This omission is significant because respondents cite that incident as the basis for its decision to widely deploy body scanners in US airports in January 2010. AR at 069.004; AR at 105.001.

D. Implementation of FBS

Respondents acknowledge that the TSA made the decision to deploy FBS for primary screening in 2009, Resp't Br. at 19, but do not provide any statutory or regulatory basis for that change in agency practice that contradicted the agency's earlier assurances that the pilot program involved the use of body scanners would be for secondary screening." AR at 010.001 (describing the testing of passenger imaging technology as a "voluntary alternative to a pat-down during second screening.") Regarding public support for the program, respondent has provided

two polls, one which immediately followed the trouser bomb incident, while failing to note that public support has diminished over time and that the public opposition has correlated with the actual experience of those who undergo the TSA's new screening procedure. *61% Oppose Full Body Scans and TSA Pat Downs; 48% Will Seek Alternative to Flying*, Zogby International, Nov. 23, 2010. Nate Silver, "The Full-Body Backlash," N.Y. Times. Nov. 15, 2010.[2] Respondents also fail to note the thousands of complaints the TSA has received from air travelers regarding the program.

STANDARD OF REVIEW

In addition to the legal dispute, 49 U.S.C. § 46110(c); 5 U.S.C. § 706(2)(A), there is a significant dispute regarding the facts in this matter. Findings of fact by the Administrator are conclusive only if supported by "substantial evidence." 49 USC § 46110(c). Petitioners have routinely cited to the actual technical description of the screening devices, AR 051, and to the statements and declarations of those subject to the searches, while respondents have cited to their own statements, policies, and even recharacterized the FBS program as "Advanced Imaging Technology (AIT)." In assessing the record, greater weight should be given to objective facts than to policy statements.

[2] Available at http://fivethirtyeight.blogs.nytimes.com/2010/11/15/the-full-body-backlash/.

Moreover, petitioners urge the Court to review the technical specifications of the devices, obtained by the petitioner EPIC in a prior FOIA lawsuit. Petitioners also ask the court to consider that respondent, in a separate but related matter, refused to release to petitioner the images actually generated by the devices. *EPIC v. DHS*, Case No. 09-02084 (RMU) (D.D.C.filed Nov. 9, 2009).

Finally, petitioners' characterization of this matter is more accurate than respondents'.

SUMMARY OF ARGUMENT

In 2004, the TSA was granted narrow authority to undertake a "pilot program" to "test and deploy" advanced airport checkpoint screening devices. The TSA subsequently set out specifications for devices that could store, record, and transmit naked images of traveler. Congress required that these devices be thoroughly evaluated prior to widespread deployment, and TSA assured the public that body scanners were in a pilot phase and would be deployed as an alternative for secondary screen. In 2008, the Senate Appropriations Committee imposed specific conditions on operational deployment and proscribed further deployment if appropriate privacy safeguards were not established. In 2009, the House passed legislation, 310-118, to prevent the use of these devices for primary screening. Then, in the spring of 2009, the TSA without public notice or opportunity for comment, as required by the APA, determined that body scanners would be the

primary screening technique for airports in the United States. In so doing, the agency raised a host of privacy, health, and religious concerns, and contravened several federal statutes. Pursuant to 5 U.S.C. § 553(e), petitioners and dozens of organizations petitioned the TSA to conduct a formal rulemaking on the substantial change in agency practice. The TSA failed to act on this petition, and petitioners, following revelations about the technical capabilities of the devices, petitioned the agency again, this time to suspend the program pending a formal rulemaking.

As the TSA has acted outside of its regulatory authority and with profound disregard for the statutory and constitutional rights of air travelers, the agency's rule should be set aside and further deployment of the body scanners should be suspended. 5 U.S.C. § 706(2)(C).

ARGUMENT

I. The TSA Rule is Subject to Notice and Comment

Respondents claim that "there is no 'rule' at issue here," Resp't Br. at 28, entirely disregards the limited statutory authority for the airport body scanner program, the conditions attached to the appropriations for the program, and the earlier representations made by the TSA regarding the program. 49 U.S.C. § 44925 note; S. Rep. No. 11-0396, at 60 (2008); AR 010.001. The TSA is describing its decision to routinely subject all air travelers to the digital equivalent of strip searches as if it were doing no more than changing the size of the plastic bins in

which travelers place their belongings. Under this view of its authority, the TSA could equally conclude that a complete body cavity search for all passengers "is merely the implementation of TSA's regulation that requires all passengers to be screened prior to entering the sterile area." Resp't Br. at 28. Indeed, the TSA may be on firmer ground with that claim because there is less evidence in the record that Congress was concerned about that eventuality than it was that the TSA might take it upon itself to make body scanners the primary screening technique.

Nor should respondents' assertion that "Standard Operating Procedures" constitute an adequate final order for review under 49 U.S.C. § 46110 carry much weight. The TSA SOPs are designated as Sensitive Security Information and are "not available for public inspection or copying." 49 C.F.R. § 1520.15(a). To rely on the TSA SOPs for APA review of agency decision making would effectively nullify judicial review.

TSA's decision to deploy airport body scanners for primary screening is arguably one of the most controversial agency actions in recent memory.[3] Indeed, petitioners, who have participated in many notice and comment rulemakings, are

[3] *See, e.g,* "Growing backlash against TSA body scanners, pat-downs," CNN, Nov. 14, 2010, http://edition.cnn.com/2010/TRAVEL/11/12/travel.screening/?hpt=Sbin ; "'Invasive' Airport Screening Stirs Backlash Among Airline Passengers," FoxNews, Nov. 12, 2010, http://www.foxnews.com/politics/2010/11/12/invasive-airport-screening-stirs-backlash-airline-passengers/#ixzz19TXDhjk5; "Screening Protests Grow as Holiday Crunch Looms," N.Y. Times, Nov. 16, 2010, at B4.

hard-pressed to recall any previous change in an agency practice that has elicited more widespread public attention. *See, e.g.,* "Backlash Grows vs. Full-body Scanners," USA Today, July 13, 2010, at A1.

Respondents' efforts to claim that there is no APA "rule" at issue and no requirement for notice and comment are simply not persuasive. In *Ass'n of Irradiated Residents v. EPA*, 494 F.3d 1027 (D.C. Cir. 2007), for example, respondents note that this Court determined that the agreements that the agency entered into with the goal of seeking compliance with a statute, *Id.* at 1033, did not constitute a "rule." As the Court explained, the "exercise of EPA's enforcement discretion are not reviewable by this court," *Id.* at 1028, but there is no exercise of enforcement discretion at issue in this matter; it is the change in agency practice, which is not in dispute, that is at issue.

Acknowledging that the TSA's action may indeed have constituted a rule, Resp't Br. at 32, respondent DHS still claims it would not be subject to notice and comment under a variety of theories, none of which are persuasive. First, respondents assert that this is an "interpretative rule," § 553(b)(A), that does not have the force or effect of law. But the TSA's "clarification" ignores the statutory provision that describes these checkpoint screening devices as a "pilot program" that the TSA shall "deploy and test." 49 U.S.C. § 44925 note. An agency pronouncement much be treated as a "legislative" rule subject to notice and

comment rulemaking if the rule effectively amends a prior legislative rule. *American Mining Congress v Mine Safety and Health Admin.*, 995 F.2d 1106, 1112 (D.C. Cir 1993). That is the case here.

Second, respondents assert this is a "general statement of policy" exempt from APA rulemaking requirements. 5 U.S.C. § 553(b)(A). This fails for the same reason as the claim above and for others as well. The exercise of legislative power cannot be a general statement of policy. In *Nader v. Butterfield*, 373 F.Supp. 1175 (D.D.C. 1974) the court held that the decision of the Federal Aviation Administration ("FAA") to deploy X-ray scanners in airport terminals was not a "general statement of policy." On facts very similar to this case, the court found that a new directive "marked a significant departure from the prior requirements, and, in effect cleared the way for airlines to eliminate the previously observed safety practices of physical visual hand baggage searches in favor of x-ray systems which met certain FAA criteria." *Id.* The court further stated, "The fact that the only government action on this subject takes the form of an internal memorandum does not dispense with the central issue of whether the practice established is subject to rulemaking. If the underlying policy requires adherence to the APA, those requirements cannot be circumvented by FAA's failure to formally promulgate its position."

Further, the agency's actions impact the rights and obligations of air travelers who are now subject to the rule. The Court need not determine at this point whether the agency's action violates the constitutional and statutory rights of air travelers, as petitioners allege, to note this action constitutes a present day "binding effect" that "constrains the agency's discretion." *McLouth Steel Products Corp. v. Thomas,* 838 F.2d 1317, 1320 (D.C. Cir. 1988). The agency has committed itself to the rapid deployment of airport body scanners, without authorization from Congress.[4] This is not a "general statement of policy."

Third, respondent reaches for § 553(b)(A) language that exempts a "rule of agency organization, practice, or procedure" from notice and comment rulemaking. *See generally American Hospital Association v. Bowen,* 834 F.2d 1037 (D.C. Cir. 1987). But *American Hospital* does not help the government's case. That court said, "The distinctive purpose of § 553's third exemption, for 'rules of agency organization, procedure or practice,' is to ensure "that agencies retain latitude in organizing their *internal* operations." *Batterton v. Marshall*, 648 F.2d 694, 707 (D.C. Cir. 1980) (emphasis added). *Id* at 1047. *See also*, *Pickus v. United States*

[4] "As of September 17, 2010, TSA has deployed 224 AIT machines to 56 airports nationwide, and our goal is to have nearly 1,000 AIT machines deployed by the end of Calendar Year 2011." Statement of John S. Pistole Administrator Transportation Security Administration U.S. Department of Homeland Security Before the Subcommittee on Transportation Security and Infrastructure Protection Committee on Homeland Security United States House of Representatives September 23, 2010.

Board of Parole, 507 F.2d 1107, 1113 (D.C. Cir. 1974). As the deployment of body scanners does not concern the internal operations of the agency, but does directly affect the rights of those over whom the agency exercises authority, the order does not constitute a "rule of agency, organization, practice, or procedure."

Acknowledging that the agency may have engaged in "a procedural error in not responding appropriately to petitioner's request for APA rulemaking," Resp't Br. at 42, Respondent nonetheless urges this court to permit the continued deployment of airport body scanners as the primary screening technique in US airports. The government further asserts that this technology is "a crucial means of protecting the travelling public from catastrophic harm," Resp't Br. at 42, but provides no support whatsoever for this contention.

Ultimately, the government seeks to avoid any meaningful APA review. It reserves the right to invoke the APA's "good cause" exception, 5 U.S.C. § 553(b)(B) if "it chooses to do so." Resp't Br. at 43. It does not want a rulemaking that will constrain its action. It has concluded that the rulemaking contemplated by petitioners "would undermine the agency's ability to perform its mission." Resp't Br. at 44. It is a federal agency, in its view, that is no longer subject to the APA.

II. TSA Wrongly Denied Petitioners' Petition for a Rulemaking

As this Court has said, "In considering the agency's denial of the rulemaking petition, we 'must examine the petition for rulemaking, comments pro and con . . .

and the agency's explanation of its decision to reject the petition.'" *Defenders of Wildlife v. Gutierrez*, 532 F.3d 913, 919 (D.C. Cir. 2008) (quoting *American Horse Prot. Ass'n. v. Lyng,* 812 F.2d 1, 4 (D.C. Cir. 1987)). Moreover, "an agency's interpretation of its own regulation is entitled to substantial deference, unless plainly erroneous or inconsistent with the regulation." *Thomas Jefferson Univ. v. Shalala*, 512 U.S. 504 (1994) (internal quotation marks omitted). However, an agency may not "evade notice and comment requirements by amending a rule under the guise of reinterpreting it." *Envtl. Integrity Project v. EPA*, 425 F.3d 992, 995 (D.C. Cir. 2006); *Devon Energy Corp. v. Kempthorne,* 551 F.3d 1030, 1037 (D.C. Cir. 2008).

Respondents seek to evade notice and comment rulemaking requirements in the manner prohibited by this Court in *Envtl. Integrity Project* and *Devon Energy Corp*. The TSA's authority to screen air travelers derives from two federal statutes. 49 U.S.C. § 44901; 49 U.S.C. § 44903. Pursuant to this statutory authority, the agency promulgated a regulation requiring air travelers to "submit to the screening and inspection of his or her person and accessible property …" 49 C.F.R. § 1540.107. There is no dispute that this regulation was subject to APA rulemaking requirements. 67 Fed. Reg. 8340-01 (Feb. 22, 2002); 67 Fed. Reg. 41635-01 (June 19, 2002); 73 Fed. Reg. 64018-01 (Oct. 28, 2008). And it is clear that the respondents' body scanner rule amends Section 1540.107, imposing new legal

obligations on travelers. Therefore, the agency wrongfully denied Petitioners' petition for a rulemaking in an attempt to evade notice and comment requirements by amending a rule under the guise of reinterpreting it.

Oddly, respondents state that a petition to suspend the primary deployment of airport body scanners is not a "petition for the issuance, amendment, or repeal of a rule," 5 U.S.C. § 553(e), though the agency does elsewhere concede that it deployed airport body scanner for primary screening. Respondents further claim that a "rational explanation" for its non-action is sufficient, but that argument collapses if the agency exercised legislative power in the promulgation of a rule and was thereby required to undertake a rulemaking. 5 U.S.C. § 551(4).

II. FBS is an Unreasonable Search

Respondents' defense of the constitutionality of this search relies primarily on *Illinois* v. *Lidster*, 540 U.S. 419 (2004). Resp't Br. at 47. As respondents point out, "suspicionless checkpoint searches are permissible when a favorable balance is struck between 'the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual.'" *Lidster* at 427. Resp't Br. at 46. But *Lidster* is easily distinguishable.

Lidster concerned a seizure of an individual not under suspicion, who was asked to answer only a few questions. This Court has said that *Lidster* does not

apply to checkpoint cases in which there is suspicion and individuals are searched. In those circumstances, courts have looked to *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000). As this Court explained in *Mills v. District of Columbia* 571 F.3d 1304 (D.C. Cir. 2009), concerning a checkpoint program ("NSZ") designed to detect evidence of criminal conduct

> *Lidster* is unlike either one [this search or *Edmond*]. The police in *Lidster* were investigating a crime that they knew to have occurred. They were not looking for suspects. As the *Lidster* Court stated, "information-seeking highway stops are less likely to provoke anxiety or to prove intrusive," than the investigative checkpoint considered in *Edmond*. As the Court stressed, "[f]urther, the law ordinarily permits police to seek the voluntary cooperation of members of the public in the investigation of a crime." . . . In short, the NSZ stop has nothing in common with the stop upheld in *Lidster* and everything in common with the unconstitutional stop in *Edmond*." (Internal citations omitted).

Id. at 1331.

This Court has also emphasized the specific problem with relying on the *Lidster* analysis when the matter at issue is the physical search of a person. In *United States v. Askew*, 529 F.3d 1119, 1135 (D.C. Cir. 2008), the Court rejected the government's contention that it should follow a *Lidster* balancing test when it had obtained evidence by removing a person's jacket. As the *Askew* court explained:

> [T]he cases relied on by the Government to support its assertion that the reasonableness balancing test provides the means by which we should assess the unzipping of appellant's jacket are inapt in that they do not involve searches. Rather, these cases simply stand for the proposition that, in certain situations, a seizure -- if limited enough in scope -- may be found reasonable

> though based on something other than probable cause to believe that criminal activity is afoot. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 124 S. Ct. 885, 157 L. Ed. 2d 843 (2004).

Id. at 1135.

As the Supreme Court itself explained in *City of Indianapolis v. Edmond*, 531 U.S. 32, 51 (2000), "We cannot sanction stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime." *Edmond* at 44. Significantly, in *Edmond*, the Court also considered the possible use of a checkpoint to thwart a terrorist attack, and still noted that it should be "appropriately tailored" and threat of attack should be "imminent." *Id*. at 44.

Respondents' additional authority is also not persuasive. In *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006), the Second Circuit upheld the random inspection of bags on New York subways based on a four factor test: (i) The government interest is immediate and substantial; (ii) A subway rider has full expectation of privacy in his containers; (iii) The search is minimally intrusive; and (iv) the program is reasonably effective. *Id.* 271-74. The court also noted that riders could decline inspection by leaving the station. *Id*. at 275. While the first two factors of the *MacWade* test favor the government, the second two do not. Moreover, unlike subway riders, airline passengers are subject to security protocol

and may not leave an airport terminal. TSA, Enforcement Sanction Guidance Policy.[5]

The failure to establish the effectiveness of these devices also weighs heavily on the determination as to whether this is a reasonable practice under the Fourth Amendment. *Compare Delaware v. Prouse*, 440 U.S. 648, 660 (1979), *with Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 454-55 (1990); *see also Edmond*, 531 U.S. at 51. Following *Prouse*, this Court has said "a checkpoint, in addition to having a legitimate primary purpose, must also "promote the state interest in a 'sufficiently productive' fashion.'" *United States v. McFayden*, 865 F.2d 1306, 1311-12 (D.C. Cir. 1989) *quoted in United States v. Davis,* 270 F.3d 977, 982 (D.C. Cir. 2001); *see also United States v. Bowman,* 496 F.3d 685, 694 (D.C. Cir. 2007) (" . . . as in *Davis*, the district court made no finding that either the roadblock, or the program as a whole, was an effective means of furthering the purpose of vehicular regulation. Nor was there any evidence that would have permitted the court to make such a finding.")

As respondents claim that petitioners have "selectively quoted" *United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2005) to establish the proposition that airport searches are reasonable if they escalate in invasiveness only after a lower

[5] Available at http://www.tsa.gov/assets/pdf/enforcement_sanction_guidance_policy.pdf.

level of screening discloses a reason to conduct a more probing search, Pet. Br. at 31-32, here is the relevant text of the opinion by then-Judge Alito in *Hartwell*:

> [T]he procedures involved in Hartwell's search were minimally intrusive. 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 and had his bag x-rayed, two screenings that involved no physical touching. Only after Hartwell set off the metal detector was he screened with a wand -- yet another less intrusive substitute for a physical pat-down. And only after the wand detected something solid on his person, and after repeated requests that he produce the item, did the TSA agents (according to Hartwell) reach into his pocket."

436 F.3d at 180. (Internal citations omitted.) Judge Alito is describing an escalating search procedure, which is almost the antithesis of subjecting all travelers at the outset to full body scans by X-ray devices. *See also* Jeffrey Rosen, "The TSA is invasive, annoying – and unconstitutional," Wash. Post, Nov. 28, 2010, at B4 ("As currently configured in U.S. airports, the new full-body scanners fail all of Alito's tests.")

Remarkably, respondents contend that "the public nature of the scan limits the possibility for abuse." Resp't Br. at 51. This claim follows an earlier description of one TSO sitting in a concealed, remote location secretly instructing another TSO, standing in front of the subject, which areas of the subject's body to inspect more closely. Resp't Br. at 19. The individual subjected to this surreptitious, x-ray screening technology has no idea what image is displayed to the TSO, captured by the device, or saved for later viewing. Respondents have

borrowed a critical insight from then-Judge Alito in *Hartwell*, 436 F.3d at 181, who was describing the physical search of a passenger that could be viewed by others in a public space, and drawn exactly the wrong conclusion.

At issue in this case is a uniquely surreptitious and intrusive search, one that gives the government the ability to observe individuals stripped naked and to examine their bodies in close detail. "We cannot conceive of a more basic subject of privacy than the naked body. The desire to shield one's unclothed figured from view of strangers, and particularly strangers of the opposite sex, is impelled by elementary self-respect and personal dignity." *York v. Story*, 324 F.2d 450, 455 (9th Cir. 1963). *See Safford Unified Sch. Dist. #1 v. Redding,* 129 S. Ct. 2633, 2643 (2010). ("The meaning of such a search, and the degradation its subject may reasonably feel, place a search that intrusive in a category of its own demanding its own specific suspicions.") Even respondents' representations that the images may not be personally identifiable at the time they are obtained does not resolve the matter. In *Northwestern Memorial Hospital v. Ashcroft,* 362 F.3d 923 (7th Cir. 2004), the Seventh Circuit considered the effectiveness of techniques to conceal the identities of women, who had received late-term abortions, contained in medical records sought by the government. The government argued that the redaction of the personally identifiable information would eliminate any privacy concerns. *Id*. at 927. The court found the government's assurances unpersuasive.

Judge Posner stated "Even if all the women whose records the government seeks know what 'redacted' means, they are bound to be skeptical that redaction will conceal their identity from the world." *Id.* at 929. Judge Posner went on to say:

> Even if there were no possibility that a patient's identity might be learned from a redacted medical record, there would be an invasion of privacy. Imagine if nude pictures of a woman, uploaded to the Internet without her consent though without identifying her by name, were downloaded in a foreign country by people who will never meet her. She would still feel that her privacy had been invaded.

Id. at 929.

III. VPPA Claim

Respondents contend that petitioners' claim that the agency has violated the Video Voyeurism Prevention Act ("VPPA"), 18 U.S.C. § 1801, should not be heard by this court and, if heard, will fail on the merits. Both assertions are wrong. First, respondents never "conducted a proceeding" pursuant to 49 U.S.C. § 46110(a) and therefore cannot now claim a requirement for prior objection. 49 U.S.C. § 46110(d). Second, there is the "reasonable ground" that the federal law that regulates "video voyeurism" is relevant to the agency's current conduct. 49 U.S.C. § 46610(d).

As to the merits, TSA's action is not permissible under the VPPA for two reasons. First, a body scanner search is not "lawful." 18 U.S.C. § 1801(c). It violates the right of air travelers to be free from unreasonable search or seizure. IV

Amend. U.S. Const. Second, the TSO's are not engaged in "law enforcement, correctional, or intelligence activity." 5 C.F.R. § 831.902; TSA, TSA Management Directive No. 1100.88-1; *compare with* 49 U.S.C. §§ 44903, 44917 (Federal Air Marshals). TSA Deputy Administrator Gale Rossides has stated that TSA has no interest in giving screeners law-enforcement power. Thomas Frank, "TSA's new policelike badges a sore point with real cops," USA Today, June 16, 2008.[6] Further, the VPPA law enforcement exception attaches to individuals and not to agencies. As the House Committee Report accompanying the legislation, explains "New §1801(c) provides exceptions for persons lawfully engaged in law enforcement or intelligence activities." H. Rep. 108-504 at 5. The VPPA is intended to cover the conduct of public transportation officials. 108th Congress, 2nd Session, 150 Cong. Rec. S 11876 (Dec. 7, 2004).

IV. Privacy Act Claim

The Privacy Act requires "each agency that maintains a system of records" to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records." 5 U.S.C. § 552a(e)(4). Respondents contend that the introduction of body scanners raises no such obligations because "there is no possible way" to link an image with passenger

[6] Available at http://www.usatoday.com/travel/flights/2008-06-15-tsa-badges_N.htm.

data. Resp't Br. at 55. That is false for multiple reasons. First, TSA requires a passenger to provide full name, date of birth, and gender when the individual makes a reservation for a "covered flight." 49 C.F.R. § 1540.107(a)(b)(1), 49 C.F.R. § 1560. These records are stored in a name-retrievable fashion by the TSA in the "Secure Flight" database and retained for up to ninety-nine years. DHS, Secure Flight Privacy Impact Assessment, Oct. 21, 2008 at 14.[7] Second, TSA requires passengers to carry and present an identification document containing the same information in the Secure Flight database prior to boarding an aircraft. 49 C.F.R. § 1540.107(a)(b)(2). The TSA visually matches air travelers' photo ID cards with their boarding passes when travelers pass through airport security checkpoints. AR 019. The TSA scans air travelers' boarding passes, collecting air travelers' personal information, when travelers pass through airport security checkpoints that are equipped with paperless boarding pass scanners. AR 128. Moreover, the TSA observes and video records all passengers as they proceed though airport screening. Further, the body scanner generates a time-stamped audit log, maintained by the TSA, that can be readily linked with the time-stamped video log, also maintained by the TSA.

As respondent TSA has the ability to link images of naked traveler with passenger data that exists in a Privacy Act system of records, 72 Fed. Reg. 48392

[7] Available at http://www.tsa.gov/assets/pdf/nprm_pia.pdf.

(Aug. 23, 2007), the agency should have issued a revised System of Records Notice ("SORN"). 5 U.S.C. § 552a(e)(4).

The agency has effectively conceded as much. The decision of the DHS Chief Privacy Officer to conduct a Privacy Impact Assessment means that the agency had in fact either engaged in activity that constituted a rule or that involved the collection of personal information, subject to the Privacy Act. 6 U.S.C. § 142(4). Nor is this concern speculative. The TSA had previously exceeded its authority to collect passenger data for this precise database. *See* DHS Privacy Office, Secure Flight Report, Dec. 2006 at 10-13.

V. HSA Claim

Petitioners contend that the DHS Chief Privacy Officer ("CPO") has failed to uphold her statutory mandate to protect the privacy of Americans with regard to the deployment of new technologies. 6 U.S.C. § 142(a)(1). Respondents answer that the CPO has "continued to monitor this subject" and has "also striven for maximum transparency in notifying the public with respect to changes" regarding the program. Resp't Br. at 56. Respondents conclude that because "the DHS Privacy Officer reached a different conclusion than petitioners does not mean she has been derelict regarding this important matter." *Id.* But the question is not whether the DHS CPO agrees or disagrees with petitioner; the question is whether she has discharged her statutory obligation.

The House report accompanying the establishment of respondent agency DHS made clear that the DHS Privacy Officer would be "responsible for assuring that all forms of technologies, in addition to information technologies, are not employed by DHS in any way that erodes citizens' privacy protections." Sec. 205, 107 H. Rpt. 609 (2002). "Guaranteeing that homeland security is achieved within a framework of law that protects the civil liberties and privacy of the United States citizens is essential." *Id.* It is difficult to imagine a more intrusive use of new technology than one that reveals the naked human body to public officials.

VI. RFRA Claim

Respondents contend that petitioners lack standing to argue that the agency's practices, which substantially burden the free exercise of religion, violate the Religious Freedom Restoration Act ("RFRA"), 42 U.S.C. § 2000bb *et seq*, and that even if petitioners have standing, the claim would not succeed. Both of these arguments fail.

First, respondents have previously replied to petitioners' RFRA claim on the merits without suggesting that petitioners lacks standing. Opp. to Emer. Mot. at 8-9. Second, the objections to the agency's action set out in the First EPIC Petition and the Second EPIC Petition include the RFRA Claims. EPIC Petition to DHS Requesting Stay of Agency Rule at 1, 7. Third, religious organizations, including the Council on American Islamic Relations ("CAIR") and the Muslim Legal Fund

of America, signed the Second EPIC Petition. 49 U.S.C. § 46110(d). Fourth, petitioner Nadhira Al-Khalili is herself a devout Muslim, a frequent traveler, and legal counsel for the CAIR. Petitioners have multiple reasons to raise the RFRA claim.

As for Respondents' claim that petitioners must meet the "constitutionality standing requirements of injury, causation, and redressability," Resp't Br. at 60, respondent previously explained that (1) the injury is the respondents' violation of several federal laws and the federal Constitution, and (2) causation is not in dispute. Pet. Br. at 40-41. As for redressability, petitioners had merely asked Respondent to "revise its airport screening programs to comply with federal laws," *Id.* but since Respondent has chosen to pursue this point, petitioner points out that the Court could also impose sanctions under various federal statutes. *See, e.g.,* 18 U.S.C. 1801(a); 42 U.S.C. § 2000bb-1(c) ("A person whose religious exercise has been burdened in violation of this section may assert that violation as a claim or defense in a judicial proceeding and obtain appropriate relief against a government."); *see Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971) (Harlan, J., concurring) ("federal courts do have the power to award damages for violation of "constitutionally protected interests" . . . .)

The government states "there is no constitutional right to travel by any means, including air," Resp. Br. at 62, but it is not the burden on the right to travel

that is at issue, it is the burden on the free exercise of religion. A "regulation is a substantial burden if it forces a person to engage in conduct that his religion forbids or prevents him from engaging in conduct his religion requires." *See Henderson v. Kennedy*, 253 F.3d 12, 16 (D.C. Cir. 2001). *Boardley v. U.S. Dep't of Interior*, 605 F. Supp. 2d 8, 14 (D.D.C. 2009), *rev'd on other grounds*, 615 F.3d 508, 523 (D.C. Cir. 2010). The government "may substantially burden a person's exercise of religion only if it demonstrates that application of the burden to the person-- . . . (2) is the least restrictive means of furthering that compelling governmental interest." 42 U.S.C § 2000bb-1(b). As this Court recently stated "[t]he statute makes clear that "the term 'demonstrates' means meets the burdens of going forward with the evidence and of persuasion." *Potter v. District of Columbia,* 558 F.3d 542, 546 (D.C. Cir. 2009). As the District had failed to meet that evidentiary burden, the court ruled in favor of the petitioners. *See also*, *Sample v. Lappin,* 424 F. Supp. 2d 187 (D.D.C. 2006).

Here as in *Potter* and *Lappin,* the government has failed to demonstrate that it has adopted "the least restrictive means" to satisfy a compelling state interest. For this reason, the government's RFRA defense also fails.

CONCLUSION

Petitioners have explained how the TSA's decision to deploy full body scanners in US airports was an exercise of legal authority, subject to the APA, and

how this agency action has violated, and continues to violate, the constitutional and statutory rights of American air travelers. Respondents have largely conceded that the TSA action is subject to the APA, but has essentially asked this court to ignore these obligations as well as the various claims that petitioners have raised. Petitioners respectfully urge the Court to reject that result, to suspend the further deployment of these devices, to require a public rulemaking, and to grant such other relief as it finds appropriate.

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: January 6, 2011

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 contains 6,996 words, in compliance with the word limit of Rule 32(a)(7)(B)(ii).

/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 6th day of January, 2011, 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