IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

JONATHAN CORBETT, Petitioner, v. TRANSPORTATION SECURITY ADMINISTRATION, Respondent.	No. 15-15717

RESPONDENT'S OPPOSITION TO PETITIONER'S MOTION TO STAY ORDER

CERTIFICATE OF INTERESTED PERSONS

Pursuant to Eleventh Circuit Rule 26.1-1, the undersigned counsel certifies that, to the best of her knowledge, the following constitutes a complete list of the trial judge(s), all attorneys, persons, associations of persons, firms, partnerships, or corporations that have an interest in the outcome of the particular case or appeal:

Corbett, Jonathan

Mizer, Benjamin C.

Swingle, Sharon

Shih, Michael

/s/ Sharon Swingle

SHARON SWINGLE
Counsel for the United States

Petitioner Jonathan Corbett has asked this Court for a nationwide preliminary injunction barring the Transportation Security Administration (TSA) from requiring certain airline passengers posing a heightened security risk to pass through scanners equipped with advanced imaging technology (AIT). Faced with two similar motions, this Court has previously denied petitioner the extraordinary relief he seeks. Petitioner's third and latest attempt to enjoin TSA's scanning policies likewise falls well short of the stringent requirements for a preliminary injunction to issue.

First, petitioner cannot establish a substantial likelihood of success, not in the least because he lacks standing to challenge the TSA policy at issue. Second, petitioner cannot show that the TSA policy threatens him with irreparable harm. Finally, the balance of equities and the public interest weigh heavily against injunctive relief. Granting petitioner's motion would pose a significant risk to the public by preventing TSA from deploying screening methods that, in the agency's expert judgment, reflect the most effective means of protecting aviation security.

STATEMENT

A. Statutory and Regulatory Background

1. Congress vests responsibility for civil aviation security in the TSA Administrator. 49 U.S.C. § 114(d). The Administrator must "assess current and potential threats to the domestic air transportation system" and take action to

protect against those threats. *Id.* §§ 44903(b), 44904(a), (e). The Administrator must specifically ensure that "all passengers and property" are screened before boarding, to prevent passengers from "carrying unlawfully a dangerous weapon, explosive, or other destructive substance." *Id.* §§ 44901(a), 44902(a).

The threat to aviation security has evolved to include the use of nonmetallic explosives and other nonmetallic threats. *See* Passenger Screening Using Advanced Imaging Technology, 78 Fed. Reg. 18,291, 18,289 (2013). In response, Congress directed TSA to give a high priority to deploying new technologies at airport security checkpoints to detect nonmetallic, chemical, biological, and radiological weapons and explosives. *See* 49 U.S.C. § 44925(a). Per that directive, TSA has used AIT scanners as a primary screening method since October 2010. *See Corbett v. TSA*, 767 F.3d 1171, 1174-75 (11th Cir. 2014). Unlike ordinary metal detectors, AIT scanners detect both metallic and nonmetallic objects on a passenger's body or concealed in clothing. *Id.* The scanners therefore address a critical weakness in the Nation's security infrastructure.

2. When TSA first implemented AIT scanners as a primary screening method, "it employed scanners that displayed the body contour of the passenger" but did not store, export, or print the images. *See Corbett*, 767 F.3d at 1175. The D.C. Circuit held that TSA's use of AIT scanners to screen passengers, and its enhanced physical pat-downs of passengers who refused AIT screening, was

lawful under the Fourth Amendment. *See Electronic Privacy Information Ctr. v. DHS*, 653 F.3d 1, 10-11 (D.C. Cir. 2011) ("*EPIC*").

As currently deployed, AIT scanners protect passengers' privacy to a greater extent than the scanners the use of which the D.C. Circuit deemed constitutional. After the D.C. Circuit decided *EPIC*, Congress mandated that any AIT scanners used for passenger screening must incorporate software "that produces a generic image of the individual being screened that is the same as the images produced for all other screened individuals." 49 U.S.C. § 44901(*l*). TSA outfitted all AIT scanners with this technology—called "automated threat recognition"—by May 2013. Consequently, AIT scanners no longer display the body contour of scanned passengers. Rather, each scanner notifies TSA agents about potential concealed threats by highlighting those areas on a generic outline of a person, which image is shown on an attached monitor. *See Corbett*, 767 F.3d at 1175; Privacy Impact Assessment Update for TSA Advanced Imaging Technology, DHS/TSA/PIA-032(d), at 2 (Dec. 18, 2015) (attached as Exhibit 1) (displaying a sample figure). AIT scanners equipped with automated threat recognition software do not collect any personally identifiable information, nor do they display an individual image every time a passenger passes through them. *See, e.g.*, Exh. 1 at 4. Rather, the software temporarily overlays the location of potential threats onto a generic outline. *Id.*

This Court has held that AIT scanners equipped with automated threat recognition software "effectively reduce the risk of air terrorism" while "pos[ing] only a slight intrusion on an individual's privacy." *Corbett*, 767 F.3d at 1181. TSA's use of such scanners is "a reasonable administrative search under the Fourth Amendment." *Id.* at 1179.

3. TSA initially deployed AIT scanners as a primary screening method without public rulemaking, *see EPIC*, 653 F.3d at 4, but the D.C. Circuit held that notice-and-comment rulemaking was required, *id.* at 8. The court remanded the rule to TSA but did not vacate it, "due to the obvious need for * * * TSA to continue its airport security operations without interruption." *Id.* at 11. As a result, TSA continues to deploy AIT scanners at checkpoints while it undertakes the notice-and-comment process.

TSA issued a notice of proposed rulemaking on March 26, 2013. Passenger Screening Using Advanced Imaging Technology, 78 Fed. Reg. 18,287 (2013). "The proposed rule codifies the use of AIT to screen individuals at aviation security screening checkpoints." *Id.* at 18,289. The preamble to the proposed rule notes that "AIT screening is currently optional," but the proposed rule did not mandate that any passenger must be permitted to opt out of AIT screening. To the contrary, it preserved TSA's flexibility to require AIT screening where warranted by security considerations. *See* 78 Fed. Reg. at 18,302 (proposing a regulatory

amendment providing that "[t]he screening and inspection described in (a) *may* include the use of advanced imaging technology") (emphasis added).

TSA invited public comment on a host of issues, including "the ability of passengers to opt-out of AIT screening" under the proposed rule. 78 Fed. Reg. at 18,294. The public took full advantage of that opportunity: TSA has received over 5,500 comments to date. *See* http://www.regulations.gov, Docket ID: TSA-2013-0004. Some commenters worried that the proposed rule would allow the agency to make AIT screening mandatory. *See* Comments of the Competitive Enterprise Institute and Robert L. Crandall, at 5-6 (June 24, 2013); *see also* Comments of Jim Harper, John Mueller and Mark Stewart of the Cato Institute, at 8-10 (June 21, 2013) (criticizing the proposed rule as vague and insufficient to bind TSA). Other commenters criticized the proposed rule for *not* making AIT screening mandatory. *See, e.g.*, Comment of James L. Bareuther (Apr. 16, 2013); *cf. Ruskai v. Pistole*, 775 F.3d 61, 81 (1st Cir. 2014) (describing petitioner's argument that TSA should be required to use AIT scanners instead of metal detectors). TSA expects to publish its final rule in 2016.

4. The Privacy Office of the Department of Homeland Security periodically issues privacy impact assessments of TSA's screening procedures. *See* http://www.dhs.gov/publication/dhstsapia-032-advanced-imaging-technology. The most recent update, dated December 18, 2015, explains that the Privacy Office is

modifying its assessment to reflect a change TSA has made to its operating protocols regarding certain passengers' ability to opt out of AIT screening in favor of a physical pat-down. Exh. 1 at 1. TSA's revised policy clarifies that, although "passengers may generally decline AIT screening in favor of physical screening, TSA [now] direct[s] mandatory AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security." *Id.* at 3.[1]

B. Prior Proceedings

This petition for review marks *pro se* petitioner Jonathan Corbett's third attempt to enjoin some aspect of TSA's screening procedures.[2] Petitioner initially sued the United States in federal district court to challenge those procedures and moved for a nationwide injunction to prevent TSA from implementing AIT screening. *See Corbett v. United States*, No. 10-cv-24106, 2011 WL 2003529 (S.D. Fla. Apr. 29, 2011). The district court denied his motion and dismissed the action for want of jurisdiction pursuant to 49 U.S.C. § 46110. Petitioner appealed

[1] The specific security considerations that support requiring certain passengers to undergo mandatory AIT screening are Sensitive Security Information and cannot be disclosed in a public filing. Should the Court wish to review the specific criteria used by TSA, however, TSA stands ready to provide that information in an under seal, *ex parte* submission to the Court.

[2] In 2012, Corbett also sued TSA and a host of other parties for twenty-one alleged statutory and constitutional violations arising from an encounter at an airport checkpoint. The district court dismissed nineteen of his claims and granted summary judgment to defendants on the remaining two. *See Corbett v. TSA*, 568 F. App'x 690, 692 (11th Cir. 2014). This Court affirmed. *Id.*

and moved for interim injunctive relief. This Court denied that motion, *see Corbett v. United States*, No. 11-12426, Order (11th Cir. July 27, 2011), and affirmed the district court's judgment, *see Corbett v. United States*, 458 F. App'x 866, 870 (11th Cir. 2012). The Supreme Court denied petitioner's petition for a writ of certiorari. *Corbett v. United States*, 133 S. Ct. 161 (2012).

Petitioner raised the same challenge in a petition for review before this Court, and moved once more for interim injunctive relief. The Court denied that second motion because it "fail[ed] to meet the applicable standard for granting injunctive relief." *See Corbett v. TSA*, No. 12-15893, Order (11th Cir. Apr. 4, 2013). The Court then dismissed the petition as untimely, and, in the alternative, denied the petition "because the challenged screening procedure does not violate the Fourth Amendment." *Corbett*, 767 F.3d at 1184. Petitioner again petitioned for a writ of certiorari, which the Supreme Court again denied. *Corbett v. TSA*, 135 S. Ct. 2867 (2015).

Petitioner's third and latest action also takes the form of a petition for review. The petition challenges the TSA's decision to change its policy to mandate AIT screening for certain travelers as warranted by security considerations. *See* Petition for Review at 1, *Corbett v. TSA*, No. 15-15717 (11th Cir. filed Dec. 28, 2015). The petition claims that TSA's revised AIT screening policy violates the Fourth Amendment and the Administrative Procedure Act.

Petitioner has yet again moved for a nationwide injunction to bar the TSA from implementing that policy. *See* Motion To Stay Order, *Corbett v. TSA*, No. 15-15717 (11th Cir. Dec. 28, 2015). Neither filing asserts that petitioner has been subjected to mandatory AIT screening under the TSA's updated policy. Petitioner states only that he is a "frequent flyer" who "fear[s] that * * * the TSA may decide to 'force' [him] into being scanned" the next time he attempts to board an airplane. *Id.* at 21. Neither filing identifies any future travel plans, imminent or otherwise.

ARGUMENT

Petitioner has moved for a nationwide injunction barring the TSA from mandating AIT screening for certain passengers for whom security considerations weigh against allowing them to opt out. This "extraordinary remedy" is "never awarded as of right." *Winter v. NRDC*, 555 U.S. 7, 24 (2008). Rather, petitioner must "clearly establish[]" that "(1) [he] has a substantial likelihood of success on the merits; (2) irreparable injury will be suffered unless the injunction issues; (3) the threatened injury to [him] outweighs whatever damage the proposed injunction may cause the opposing party; and (4) if issued, the injunction would not be adverse to the public interest." *See ACLU of Fla., Inc. v. Miami-Dade Cnty. Sch. Bd.*, 557 F.3d 1177, 1198 (11th Cir. 2009) (quotation marks and citations omitted). Petitioner's motion fails at each turn.

1. First and foremost, petitioner cannot show a substantial likelihood of success on his petition for review. At the threshold, petitioner lacks standing to challenge the TSA policy at issue. Petitioner at no point claims that he has been subjected to mandatory AIT screening in the past. Nor can petitioner prove that he faces an imminent threat of mandatory screening in the future. His filings do not identify any future travel plans, imminent or otherwise, nor do they provide any reason why he would be subject to mandatory AIT screening due to security considerations. His petition does not even allege any facts "disclosing a substantial interest" in the challenged order—a statutory predicate for any petition for review filed under 49 U.S.C. § 46110. Petitioner asserts only that he is a regular traveler. That allegation falls well short of the showing petitioner must make to prevail: that the challenged policy inflicts a "palpable, ideally a measurable" harm to a "concrete, individual, nonideological, in short weighty, interest" that he possesses. *See Ill. Dep't of Transp. v. Hinson*, 122 F.3d 370, 371-72 (7th Cir. 1997).

Petitioner could not succeed on the merits even if this Court had jurisdiction over his petition. As to his constitutional claim, this Court has already held, in an action brought by this very petitioner, that requiring passengers to pass through an AIT scanner at an airport checkpoint constitutes "a reasonable administrative search" under the Fourth Amendment. *Corbett*, 767 F.3d at 1180. The Court explained that "the scanners effectively reduce the risk of air terrorism" by

enabling TSA agents to identify nonmetallic threat objects that ordinary metal detectors cannot detect. *Id.* at 1180-81. Any privacy concerns arising from AIT screening—already "slight" when TSA first introduced AIT screening—have been "greatly diminished" by the reality that "[t]he scanners now create only a generic outline of an individual." *Id.* at 1181. "The jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane outweighs the slight intrusion of a generic body scan." *Id.* at 1182 (quotation marks and citation omitted).

That holding controls this case. As the Court noted when rejecting petitioner's earlier challenge, "[t]he Fourth Amendment does not compel [TSA] to employ the least invasive procedure or one fancied by [petitioner]." *Id.* at 1182. The choice of how best to "'deal with a serious public danger' * * * should be left to those with 'a unique understanding of, and a responsibility for, limited public resources.'" *Id.* at 1181 (quoting *Mich. Dep't of St. Police v. Sitz*, 496 U.S. 444, 453-54 (1990)). Where, as here, TSA has concluded that certain passengers pose enough of a security risk to warrant heightened AIT scrutiny, this Court "need only determine whether the [policy] is a reasonably effective means of addressing the government interest in deterring and detecting a terrorist attack" at airports. *Id.* (citation omitted). Here, as there, "[c]ommon sense" suggests that TSA reasonably

concluded that security considerations may sometimes weigh in favor of preventing certain passengers to opt out of AIT screening. *Id.*

Petitioner's procedural claim fares no better. The narrow policy revision at issue modifies TSA's screening procedure for certain passengers for whom security considerations support AIT screening with no ability to opt out. Nothing about the revision, which does not require any passenger to undergo screening that produces an unclothed image of him or even any individualized image, "intrudes upon [the passenger]'s personal privacy in a way" that ordinary security screening procedures do not. *Cf. EPIC*, 653 F.3d at 6. Petitioner relies on incorrect facts, *see* Mot. at 5, and an outdated holding, *see EPIC*, 653 F.3d at 6, for the erroneous conclusion that passing through an AIT scanner equipped with automated threat recognition software "substantively affects the public" in a way ordinary security screening does not. Because the policy does not impose a new substantive obligation on passengers, it does not qualify as a substantive rule for which notice-and-comment rulemaking is required.

Petitioner's rejoinders do not hold water. As to standing, petitioner asserts (Mot. at 9) that his "fear" that TSA may subject him to mandatory AIT screening on some unspecified date qualifies as an injury-in-fact. But the Supreme Court has rejected the theory that "highly speculative fear" can establish Article III jurisdiction. *See Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1148 (2013).

Petitioner next asserts, without citing a single source (Mot. at 5-6), that AIT scanners create images of passengers' naked bodies and could be "program[med] * * * to display, save, e-mail, and print [those] images." This claim misrepresents or misapprehends the additional steps TSA has taken to preserve passenger privacy. As explained above, AIT scanners do not collect or store any personally identifiable information. Furthermore, the systems in use at airports are not configured to display or transmit any passenger-specific image; the software present on those systems lacks that functionality. The scanners simply overlay highlighted boxes (representing areas warranting further investigation) onto a generic image that does not vary from person to person. Even were it possible to tamper with an AIT scanner in the manner petitioner fears, petitioner has presented no evidence of any tampering with any scanner at any checkpoint in any airport. At any rate, petitioner cannot establish standing even under his mistaken factual premises. Petitioner will only be harmed if TSA subjects him to mandatory AIT screening on some unspecified date, and if in the course of that screening he encounters a scanner reprogrammed to display images the scanner cannot currently display. Petitioner's second theory of injury is thus more speculative than his first.

Petitioner lastly asserts (Mot. at 9-10) that he has been injured by TSA's alleged failure to promulgate its revised policy by way of notice-and-comment rulemaking. As we have explained, this theory rests on the erroneous premise that

TSA's policy change is a "substantive rule" that must be promulgated in that manner. The theory also fails on its own terms. Even if TSA violated the APA's procedural requirements, petitioner cannot show how that violation has "impair[ed]" any "concrete interest" in a way that would confer jurisdiction on this court. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 572-73 (1992).

In any event, it would make little sense for this Court to grant greater preliminary relief than the Court would be likely to order if petitioner were successful on his procedural challenge. Even where the D.C. Circuit held that TSA was required to conduct notice-and-comment rulemaking in order to use AIT scanners without privacy software to screen passengers, that Court declined to vacate the AIT screening policy pending such rulemaking. That rulemaking is underway, and makes clear that TSA screening "may include" the use of AIT, and expressly invites comments on passengers' ability to "opt-out of AIT screening." 78 Fed. Reg. at 18,302, 18,294. Petitioner's challenge, which effectively takes issue with the scope and timing of that rulemaking, is unlikely to succeed on the merits, and does not support the issuance of preliminary injunctive relief.

As to the merits of his constitutional claim, petitioner attempts to distinguish (Mot. at 6-7) this Court's previous holding that TSA does not violate the Fourth Amendment when it subjects passengers to AIT screening at airport checkpoints. *See Corbett*, 767 F.3d 1171. But Petitioner's argument that *Corbett* does not apply

to a policy mandating AIT screening for certain passengers posing a heightened security threat is belied by *Corbett* itself. The Court's analysis turned on AIT scanners' "self-evident" power to "reduce the risk of air terrorism" at minimal cost to privacy, not on the fact that TSA had made AIT screening optional for all passengers. *Id.* at 1181. *Corbett* therefore cannot be distinguished from this case.

The D.C. Circuit's decision in *EPIC*, 653 F.3d at 1, also does not support petitioner's position. That court discussed TSA's previous opt-out procedures in the context of a Fourth Amendment challenge to the use of a now-defunct model of AIT scanner, which produced an image of each passenger for viewing by a TSA employee. *Id.* at 10. Today's AIT scanners no longer generate a particularized image. The technological feature requiring the *EPIC* court to discuss existing opt-out procedures—that is, the impact on personal privacy of permitting a TSA employee to view a passenger-specific image—no longer exists.

2. *Irreparable injury.* Petitioner's motion for extraordinary injunctive relief fails for the independent reason that he cannot identify any irreparable injury he will suffer if an injunction is not granted.

As explained above, petitioner has not alleged any future travel plans that might expose him to any form of AIT screening. Even if travel were imminent, petitioner has not set forth any reason to believe that TSA will subject him to mandatory AIT screening under its revised policy of requiring such screening for

passengers posing heightened security risks. In either event, petitioner remains free to avoid AIT screening by foregoing airplane travel in favor of buses, trains, and automobiles. That these alternatives may be less convenient does not mean that recourse to them creates an irreparable injury. *See Town of Southold v. Town of E. Hampton*, 477 F.3d 38, 54 (2d Cir. 2007); *cf. Molloy v. Metro. Transp. Auth.*, 94 F.3d 808, 813 (2d Cir. 1996) (noting that "passengers do not possess a constitutional right to the most convenient form of travel") (quotation marks and citation omitted). In short, petitioner cannot show how allowing TSA to implement its revised screening policy would inflict any injury upon him, much less an irreparable one.

Petitioner resists this conclusion by invoking the principle (Mot. at 9) that "constitutional injuries are generally considered irreparable." But the premise of his argument—that the revised screening policy inflicts a constitutional injury—is flawed. This Court has already held that the Fourth Amendment permits TSA to deploy AIT scanners at airport checkpoints. *See Corbett*, 767 F.3d at 1180. And even if TSA's use of AIT scanners *does* violate the Fourth Amendment, petitioner must still show that the scanners will be "used on [him]" to establish irreparable injury under this principle—as his own filing acknowledges. *See* Mot. at 10. That he has failed to do.

Petitioner persists that TSA's alleged failure to conduct a separate notice-and-comment rulemaking before changing its screening policies amounts to an irreparable injury warranting injunctive relief. But a mere procedural violation does not modify the requirement that a petitioner demonstrate an irreparable injury to a concrete interest to prove his entitlement to a preliminary injunction. *Animal Welfare Inst. v. Martin*, 623 F.3d 19, 27 (1st Cir. 2010); *see Lujan v. Defenders of Wildlife*, 504 U.S. 555, 572 (1992). Here again, petitioner merely speculates that TSA will subject him to its revised screening policy.

Finding irreparable injury on procedural grounds is especially inappropriate when, as here, TSA has *already* engaged in notice-and-comment rulemaking to ventilate the issue at this petition's core: whether TSA can require certain passengers to undergo AIT screening. The proposed rule states that TSA screening "may include" the use of AIT, 78 Fed. Reg. at 18,302, and its preamble expressly requested comments "on the ability of passengers to opt-out of AIT screening," *id.* at 18,294. Several commenters objected to mandatory screening; at least one commenter endorsed mandatory screening. TSA expects to issue a final rule this year that takes these comments into account. In sum, the existing rulemaking encompasses the challenge petitioner has brought. *See Appalachian Power Co. v. EPA*, 135 F.3d 791, 816 (D.C. Cir. 1998).

3. The balance of equities and the public interest weigh decisively against petitioner's demand for injunctive relief. *See Winter*, 555 U.S. at 24 ("[C]ourts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction.") (quotation marks omitted). "[T]here can be no doubt that preventing terrorist attacks on airplanes is of paramount importance." *Corbett*, 767 F.3d at 1180 (quoting *United States v. Hartwell*, 436 F.3d 174, 179 (3d Cir. 2006)). Effective aviation security screening unquestionably furthers that goal, as does the use of AIT scanners to detect nonmetallic threats that ordinary metal detectors cannot. *Id.* Preventing TSA from requiring certain passengers posing a heightened security risk to undergo AIT scanning would undermine national security and jeopardize public safety.

This Court has twice refused this petitioner's invitations to bring AIT scanning to a halt. *Corbett*, No. 12-15893, Order (11th Cir. Apr. 4, 2013); *Corbett*, No. 11-12426, Order (11th Cir. July 27, 2011). Every other court to consider the question has reached the same conclusion. *See EPIC v. DHS*, No. 10-157, Order (D.C. Cir. Sept. 1, 2010); *Blitz v. Napolitano*, No. 1:10-cv-930, Transcript of 12/10/10 Hearing, at 53-58, and 12/13/2010 Order (M.D.N.C.). Petitioner's latest attempt to enjoin TSA's screening procedures should be treated no differently.

CONCLUSION

For these reasons, the motion should be denied.

Respectfully submitted,

/s/ Sharon Swingle
SHARON SWINGLE
MICHAEL SHIH
(202) 353-2689
Attorneys, Appellate Staff
Civil Division
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Room 7250
Washington, D.C. 20530
Counsel for the United States

JANUARY 2016

EXHIBIT 1

Privacy Impact Assessment Update
for

TSA Advanced Imaging Technology

DHS/TSA/PIA-032(d)

December 18, 2015

Contact Point
Jill Vaughan
Assistant Administrator
Office of Security Capabilities
OSCCommunications@dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) has deployed Advanced Imaging Technologies (AIT) for operational use to detect threat objects carried on persons entering airport sterile areas. AIT identifies potential threat objects on the body using Automatic Target Recognition (ATR) software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt opt-out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers. TSA does not store any personally identifiable information from AIT screening.

Introduction

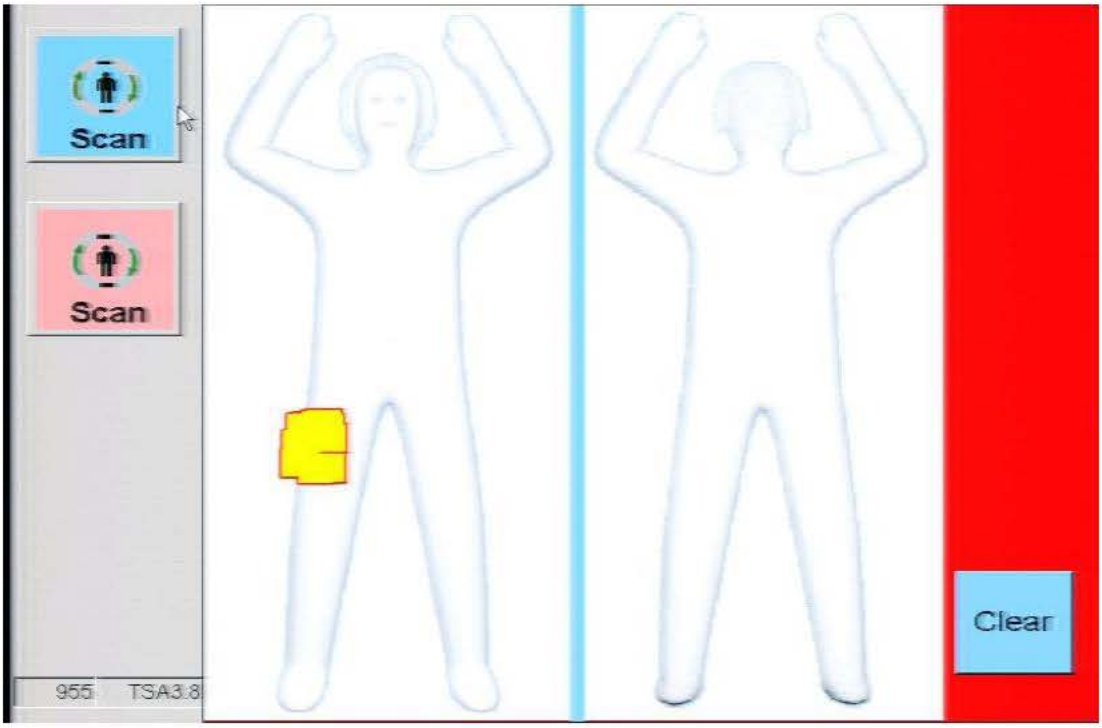
Under the Aviation and Transportation Security Act (ATSA),[1] TSA is responsible for security in all modes of transportation, and must assess threats to transportation, enforce security-related regulations and requirements, and ensure the adequacy of security measures at airports and other transportation facilities. TSA has deployed AIT for operational use to detect threat objects carried on persons entering airport sterile areas.[2] AIT identifies potential threat objects on the body using ATR software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA currently uses AIT equipped with ATR to quickly, and without physical contact, screen passengers for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. ATR software identifies objects on the body and highlights the location of the object with bounding boxes on a generic figure.[3] ATR eliminates the need for a remote image since it is a generic image that can be presented on a monitor connected to the AIT and co-located with the officer assisting the screened individual. The individual will undergo physical screening if ATR alarms for the presence of an object.

[1] Pub. L. 107-71

[2] "Sterile area" is defined in 49 CFR 1540.5 and generally means an area of an airport with access limited to persons who have undergone security screening by TSA.

[3] For additional information, *see* DHS/TSA/PIA-032 TSA Advanced Imaging Technology and associated updates, *available at* www.dhs.gov/privacy.

A sample image from a system using ATR appears below:



Storage of images

The AIT devices at airports do not have the ability to store images..[4] The ATR generic image is maintained on the monitor only for as long as it takes to resolve any alarms. The AIT equipment does not generate or retain an underlying image of the individual.

What to expect

Because the ATR software replaces the individual's image with that of a generic figure, the monitor will be co-located with the individual being screened. The screening officer will view both the individual and the ATR image. If there is an alarm, the physical screening will target the location indicated by the ATR software. If there are multiple alarms, the individual may receive a full screening.

[4] Initial versions of AIT were manufactured with storage functions that TSA required manufacturers to disable prior to installation at the airport. Current versions of the software installed at airports do not include any storage function to disable, and eliminate the need to perform the disabling of the storage function.

Reason for this Update

TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices set out in the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy.

In response to this obligation, the DHS Privacy Office has developed a set of Fair Information Practice Principles (FIPPs) from the underling concepts of the Privacy Act that encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure. Given the particular technologies and the scope and nature of their use, TSA used the DHS Privacy Office FIPPs PIA template.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

TSA has published information on AIT technologies on its website (www.TSA.gov), and published an original PIA on AIT in January 2008 with subsequent updates reflecting operational or technology changes.[5] In 2013, TSA published a Notice of Proposed Rule Making on the use of AIT in screening operations which received more than 5500 comments from the public. TSA expects to publish its Final Rule in 2016. This PIA update reflects TSA's continued transparency on its use of AIT.

[5] For all TSA Privacy Impact Assessments, please visit http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individuals undergoing screening using AIT generally will have the option to decline an AIT screening in favor of physical screening. Given the implementation of ATR and the mitigation of privacy issues associated with the individual image generated by previous versions of AIT not using ATR, and the need to respond to potential security threats, TSA will nonetheless mandate AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII, to include images, and specifically articulate the purpose or purposes for which the PII is intended to be used.

TSA is responsible for security in all modes of transportation, including commercial aviation.[6] Congress directed TSA to conduct research, development, testing, and evaluation of threats carried on persons boarding aircraft or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction.[7] AIT technologies are being used to identify prohibited items, particularly non-metallic threat objects and liquids secreted on the body. ATR software identifies the location of the potential prohibited item on a generic figure. Because of the greater privacy protections provided by a generic figure, the image monitor for ATR is co-located with the AIT so that the screening officer can view it.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

TSA does not collect PII with this technology. AIT with ATR does not generate an individual image but rather overlays the location of objects on a generic image.

---

[6] 49 U.S.C. § 114(d).
[7] 49 U.S.C. § 44912 note.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

TSA uses AIT solely for purposes of identifying objects that may be threat items. Once an alarm is resolved, the generic image is cleared from the screen, and therefore cannot be used for any other purpose or shared with anyone. Because there are no images to share, they cannot be used in any other context inside DHS or outside of the Department.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII, including images, is accurate, relevant, timely, and complete, within the context of each use of the PII.

The ATR generated image is accurate, timely, and complete and is directly relevant to the identification of threat objects. Potential threat items are resolved through a directed physical screening before the individual is cleared to enter the sterile area.

7. Principle of Security

Principle: DHS should protect PII, including images, through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

AIT data is transmitted in a proprietary format to the viewing monitor, and cannot be lost, modified, or disclosed. TSA's decision not to retain images mitigates further data storage security issues.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, including images, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

No PII is generated by AIT using ATR.

Conclusion

AIT technology improves threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical screening is uncomfortable. ATR software provides even greater privacy protections by eliminating the human image that appeared with previous AIT technologies.

Responsible Officials

Jill Vaughan
Assistant Administrator
Office of Security Capabilities

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

EXHIBIT 2

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 12-15893-A

JONATHAN CORBETT,

Petitioner,

versus

TRANSPORTATION SECURITY ADMINISTRATION,

Respondent.

On Petition for Review of a Decision of the
Transportation Security Administration

BEFORE: BARKETT, HULL and PRYOR, Circuit Judges.

BY THE COURT:

Petitioner's "Motion to Transfer to District Court" is DENIED.

Petitioner's "Motion to Stay Order" is DENIED, as his motion fails to meet the applicable standard for granting injunctive relief. See, e.g., Touchton v. McDermott, 234 F.3d 1130, 1132 (11th Cir. 2000).

Petitioner's "Motion for Leave to File Electronically" is DENIED.

EXHIBIT 3

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 11-12426-BB

JONATHAN CORBETT,

Plaintiff - Appellant,

versus

UNITED STATES OF AMERICA,

Defendant - Appellee.

On Appeal from the United States District Court
for the Southern District of Florida

BEFORE: CARNES, HULL and MARCUS, Circuit Judges.

BY THE COURT:

Appellant's "Motion for Preliminary Injunction" is DENIED.

EXHIBIT 4

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 10-1157 **September Term 2009**

DHS-May28,2010Letter

Filed On: September 1, 2010

Electronic Privacy Information Center, et al.,

Petitioners

v.

United States Department of Homeland Security, et al.,

Respondents

BEFORE: Ginsburg, Brown, and Griffith, Circuit Judges

O R D E R

Upon consideration of the motion for stay, which the court construes as a motion for injunctive relief, the opposition thereto, and the reply, it is

ORDERED that the motion be denied. Petitioners have not satisfied the stringent standards required for an injunction pending judicial review. See Washington Metropolitan Area Transit Commission v. Holiday Tours, Inc., 559 F.2d 841, 843 (D.C. Cir. 1977); D.C. Circuit Handbook of Practice and Internal Procedures 32-33 (2010).

The Clerk is directed to enter a briefing schedule and to schedule oral argument on the first appropriate date following the completion of briefing.

Per Curiam

FOR THE COURT:
Mark J. Langer, Clerk

BY: /s/
Heather Stockslager
Deputy Clerk/LD

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF NORTH CAROLINA

JONATHAN BLITZ, MARLA TUCHINSKY, and as legal, guardians of EB, their minor child, Plaintiffs vs. JANET NAPOLITANO, Secretary of Homeland Security, and JOHN PISTOLE,Administrator Transportation Security Administration, Defendants.	Civl Action Case No. 1:10CV930 Greensboro, North Carolina December 10, 2010 2:06 p.m.

TRANSCRIPT OF MOTION FOR TEMPORARY RESTRAINING ORDER

BEFORE THE HONORABLE WILLIAM L. OSTEEN, JR.

UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiffs: Jonathan Blitz, Esq.
Jonathan Blitz, Attorney At Law
PO Box 61764
Durham, NC 27715

For the Defendants: Carlotta P. Wells, Esq.
Joseph W. Mead, Esq.
U.S. Department of Justice
20 Massachusetts AVE., NW, ROOM 7152
Washington, DC 20530

Gillian Flory,Esq.
Transportation Security Administration

Gill P. Beck, Esq.
Office of U.S. Attorney
PO Box 1858
Greensboro, NC 27402

I N D E X

WITNESSES: PLAINTIFF

None

WITNESSES: DEFENDANT

None

EXHIBITS: MARKED RCVD

None

Court Reporter: Joseph B. Armstrong, RMR, FCRR
324 W. Market, Room 101
Greensboro, NC 27401

Proceedings reported by stenotype reporter.
Transcript produced by Computer-Aided Transcription.

Greensboro, North Carolina

December 10, 2010

(At 2:06 p.m., proceedings commenced.)

THE COURT: All right. Good afternoon. We are here on a motion for temporary restraining order and/or preliminary injunction in 1:10CV930, Blitz versus Napolitano, I'll just say et al. for purposes of this introduction. Mr. Blitz, if you will state for the record that you are here and who is seated at your table with you.

MR. BLITZ: Yes, Judge. Good afternoon, Jonathan Blitz here on my own behalf and also on behalf of Marla Tuchinsky, who's my wife, and also we're here on behalf of EB who is our minor child as described in the pleadings.

THE COURT: All right. And for the Government?

MR. BECK: Your Honor, it's my pleasure to introduce Carlotta Wells from the Federal Programs Branch Civil Division who will be making the argument today; Joseph Mead, also from Federal Programs; and Gillian Flory from Transportation Security Administration, also general counsel.

THE COURT: All right. Good afternoon to all of you. Mr. Blitz, I assume you'll be handling the argument for all the plaintiffs in the case.

MR. BLITZ: I'm the only lawyer and one of the two who can speak.

If there are no more questions?

THE COURT: All right. Let's take a recess and come back, and we'll figure out where we're going. We'll stand in recess for 15 minutes.

(At 3:24 p.m., break taken.)

(At 3:52 p.m., break concluded.)

THE COURT: All right. Mr. Blitz and Ms. Wells, I appreciate the arguments that were advanced here today. I think there's something to commend both sides. Mr. Blitz, I certainly understand your concern about secrecy which you say seems to run contrary to a lot of things our court system stands for, and I very much appreciate your confidence in the District Court to conduct an appropriate fact-finding mission. I wouldn't be quite so quick to sell the Circuit Courts short in that regard, but I do appreciate your comments in that regard.

I am going to deny the motion. I will explain my reasoning on that briefly. And then at the end of that, Mr. Blitz, depending on how you wish to proceed, I know you're traveling next week, we can talk a little bit about whether -- what your preference is in terms of procedural posture of the case if you want to proceed from here. But let me explain my reasoning, and then you can let me know what you want to do.

Presently before the Court is plaintiff's motion

for preliminary injunction, Document 4. And as I just mentioned, I conclude that the plaintiffs have not demonstrated that the extraordinary remedy of a preliminary injunction should be issued in this case, and I will therefore deny the motion for a TRO and preliminary injunction.

To obtain a preliminary injunction, the plaintiff must establish that he is likely to succeed on the merits; that he is likely to suffer irreparable harm in the absence of preliminary relief; and that the balance of equities tips in his favor; and, finally, that an injunction is in the public interest. That's Winter, 129 S. Ct. at 374.

For multiple reasons, I conclude that the plaintiffs have not shown that they are likely to succeed on the merits of their claims against defendants such that a TRO or preliminary injunction should issue.

First, it is, at best, unclear at this point whether this Court has jurisdiction to adjudicate plaintiffs' claims. When I say "at best," what I mean by that is it seems to me I do not.

By statute, a person disclosing a substantial interest in an order issued by the administrator for the Transportation Security Administration, TSA, under Part A of Subtitle 7 of Title 49 of the United States Code, which I'll refer to hereinafter as Part A, may apply for a review of

the order by filing a petition for review in the United States Court of Appeals for the DC Circuit or in the Court of Appeals of the United States for the circuit in which the person resides or has its principal place of business. That's 49 USC Section 46110(a). That statute further provides that the United States Court of Appeals has exclusive jurisdiction to affirm, amend, modify, or set aside any part of the order. That's 46110(c).

The TSA screening procedures at issue in this case are required under TSA's current standard operating procedures for checkpoint screening; that is, SOP. The SOP on this record appears to meet the criteria set forth in Section 46110(a) in that it is issued by the administrator for TSA and is apparently issued pursuant to the administrator's mandate under Part A which requires the administrator to provide for the screening of all passengers and property that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or interstate air transportation. That's 4901(a).

Thus, if the SOP constitutes an order for purposes of 49 USC Section 46110, then the Court of Appeals is the proper forum for review that the plaintiffs seek. City of Tacoma versus Taxpayers of Tacoma, 357 US at 336. In that case, the Supreme Court held that a statute vesting the

Court of Appeals with exclusive jurisdiction to review an administrative order necessarily precluded de novo litigation between the parties of all issues and hearing in the controversy and all other modes of judicial review.

While it is not entirely clear to this Court that the SOP constitutes an order under Section 46110, at this point, based on the record presently before me, I conclude that it is an order within the meaning of the statute. At a minimum, this difficult jurisdictional matter makes success on the merits less likely.

But with respect to the question of whether or not the SOP constitutes an order, the Fourth Circuit has stated that the existence of a reviewable administrative record is a determinative factor in defining an administrative decision as an order and also that the agency action must be the final disposition of the matter it addresses to be deemed an order. That's City of Alexandria versus Helms, 728 F.2d at 646.

It does seem to be clear that the administrative record does not have to be lengthy. It need only be an agency decision which imposes an obligation, denies a right, or fixes some legal relationship. Another part of the test includes the question of whether or not the order provides a definitive statement of the agency's position or -- and has a direct and immediate effect on the day-to-day business of

the party asserting the wrongdoing and envisions immediate compliance with its terms. Those are other factors in determining whether or not the SOP constitutes an order.

I find that because the SOP conclusively settles the matter of deploying the screening methods at issue in this case, the SOP is a final disposition by TSA and the SOP itself, and the documents that TSA reviewed in connection with the SOP appear to constitute a reviewable administrative record. As Pistole points out in his affidavit, there have been specific written SOPs generated by TSA.

In support of these propositions, see Green versus Brantley 981 F.2d 514; Atorie Air versus FAA, 942 F.2d 954; and Southern California Aerial Advertisers Association versus FAA, 881 F.2d 672.

Further, other Federal Courts have held that TSA actions similar to the SOP at issue in this case constitute orders under Section 46110 and, therefore, cannot be reviewed in the District Court. That's Gilmore versus Gonzales, 435 F.3d 1125; Green versus TSA, 351 F. Supp. 2d 1119.

Although plaintiffs have advanced reasonable arguments as to why the SOP should not be considered an order for purposes of Section 46110, this Court concludes in light of the foregoing authorities that plaintiffs have not

made a clear showing that this Court has jurisdiction to adjudicate their claim. See Winter 129 S. Ct. 376.

Plaintiffs have not satisfied this Court that they are likely to succeed on the merits. See Munaf versus Geren 553 US 674 wherein that Court stated a difficult question as to jurisdiction makes success on the merits more unlikely due to potential impediments to even reaching the merits, and, thus, plaintiffs are not entitled to a preliminary injunction in this case.

This Court also concludes that plaintiffs have not made the requisite clear showing that they are likely to succeed on the merits with respect to the reasonableness of the challenged screening procedures. Defendants have proffered significant evidence of the grave threats that adhere in air travel, the failure of less sensitive screening methods to identify and neutralize those threats, and the efforts by TSA to make the challenged screening procedures as minimally invasive as possible. Although plaintiffs have made sensible arguments that the challenged screening procedures are unreasonably invasive, even in light of the threats they seek to combat, at this point for purposes of a TRO or preliminary injunction, I cannot find that plaintiffs are likely to succeed on the merits or demonstrate that such is the case.

Finally, it appears to me that in the absence of

that -- let me back up. It appears to me that the plaintiffs have not made a clear showing that the requested injunction is in the public interest. Again, defendants have proffered significant evidence of the utility of the challenged screening methods and neutralizing threats of aviation-related terrorism. Given the presence of such threats and this Court's conclusion that the plaintiffs have not shown that they are likely to succeed in demonstrating violations of their constitutional rights, an injunction reducing defendants' ability to employ the challenged methods would not benefit the public at least based on the record as it exists at this preliminary stage of the proceedings.

So that, Mr. Blitz, is my ruling. I don't know whether or not -- I told you I wouldn't dismiss it, and I won't dismiss the case until you've had a chance to respond to the 12(b)(1)argument. I don't feel that that's been fully briefed at this point in time. But that's my finding, and I don't know if you have a preference as to simply denying the motion and then you may decide whether you want to proceed in the Fourth Circuit under an appeal of that order, or whether something else would be more appropriate. I'll hear from you. Do you understand my question?

MR. BLITZ: I think I do, Judge. I think I'm not going to ask you to go further than just denying the motion

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

JONATHAN BLITZ, MARLA TUCHINSKY, EB	)	
Plaintiffs,	)	
v.	)	1:10CV930
JANET NAPOLITANO, JOHN PISTOLE	)	
Defendants.	)	

ORDER

For the reason stated on the record during open-court, Plaintiffs' motion for temporary restraining order (Doc. 4) will be denied.

IT IS HEREBY ORDERED that Plaintiffs' Motion for Temporary Restraining Order (Doc. 4) is DENIED.

This the 13th day of December 2010.

William L. Osteen, Jr.
United States District Judge

CERTIFICATE OF SERVICE

I hereby certify that on January 7, 2016, I filed the foregoing motion with the Clerk of the Court by electronic delivery. I served the following party with the foregoing motion by electronic delivery and regular mail:

Jonathan Corbett
382 N.E. 191st St., #86952
Miami, FL 33179
jon@professional-troublemaker.com

/s/ Sharon Swingle
SHARON SWINGLE
Counsel for the United States