

**Statement of Jim Harper, Vice President, and Marc Scribner, Senior Fellow,
at the Competitive Enterprise Institute,
for the Record of the Hearing Entitled
“Checkpoint of the Future: Evaluating TSA’s Innovation Task Force Initiative,”
Conducted by the Transportation and Protective Security Subcommittee of the
U.S. House of Representatives’ Homeland Security Committee**

April 27, 2017

Chairman Katko, Ranking Member Coleman, and members of the subcommittee,

We are pleased to supplement the record of your hearing with our views on innovation at the Transportation Security Administration (TSA). While innovation is generally good, the TSA is not positioned to innovate well because of its failure to adhere to the requirements of the Administrative Procedure Act or to use risk assessment and cost-benefit analysis in its decision-making. Failed past efforts at innovation are symptomatic of these problems; the TSA continues to flout these basic responsibilities in the area of body scanners, for example; and we can expect more privacy-invasive technology failures if the TSA fails to adhere to the law and to sound risk management principles.

“Puffer Machines”: Innovative, but Useless

Since 2002 when airport security was nationalized in the wake of the September 11 terrorist attacks and the TSA was created, officials have struggled to identify and deploy passenger screening technologies designed to crisply address threats to aviation. Too often, this has led not only to the rollout of ineffective and expensive security technologies and procedures that thwart air travel, but to legally defective policies.

Take, for instance, the case of Explosive Trace Detection Portals (colloquially known as “puffer machines”), which blow air on passengers to search for explosives.¹ From 2004 to 2006, TSA deployed 101 puffer machines throughout U.S. airports, but phased out the units due to insufficient reliability and effectiveness.² They then sat unused in a Texas warehouse for upwards of four years before TSA was able to dispose of them.³ Congressional investigators in

¹ Eric Lipton, *Screening Tools Slow to Arrive in U.S. Airports*, N.Y. TIMES (Sep. 3, 2006), available at <http://www.nytimes.com/2006/09/03/us/03research.html>.

² JOINT MAJORITY STAFF REPORT, 112TH CONG., AIRPORT INSECURITY: TSA’S FAILURE TO COST-EFFECTIVELY PROCURE, DEPLOY, AND WAREHOUSE ITS SCREENING TECHNOLOGIES 6 (May 9, 2012), available at <https://oversight.house.gov/wp-content/uploads/2012/05/5-9-2012-Joint-TSA-Staff-Report-FINAL.pdf>.

³ *Id.*

2012 said this of TSA's procurement and deployment of puffers: "TSA rushed this untested product to deployment, ignoring internal procedures designed to prevent this type of waste."⁴ But the procurement and deployment missteps in the puffer example are dwarfed by the procedural and legal deficiencies of its rollout of advanced imaging technology (AIT), commonly referred to as "body scanners." In this case, TSA has repeatedly flouted the Administrative Procedure Act (APA) and other policies in a variety of ways, subjecting the issues to years of litigation that continues today.

A Case Study of Institutional Failure: TSA's Deployment of Body Scanners

In June 2008, TSA installed body scanning machines in ten major U.S. commercial airports.⁵ These scanners, which can see through clothing, are supposed to identify security threats capable of evading metal detectors. In the years that followed, TSA installed hundreds of these body scanners at airports nationwide. It did so without conducting sufficient analysis of this technology's costs and benefits and without following the requirements of the APA. Instead, it has strung the public and the federal courts along in legal and regulatory dispute that is now nearly eight years old.

On May 31, 2009, a coalition of public interest groups led by the Electronic Privacy Information Center (EPIC) submitted a petition pursuant to 5 U.S.C. § 553(e) asking DHS Secretary Janet Napolitano to initiate a formal rulemaking process to receive public input on TSA's use of body scanners to screen passengers at commercial airports.⁶ TSA's Acting Administrator responded to the petition with a short letter discussing how and why TSA uses body scanners.⁷ The letter did not address the request for a rulemaking.

On April 21, 2010, the EPIC-led coalition submitted another Section 553(e) petition requesting that TSA immediately suspend the purchase, deployment, and operation of body scanners and arguing that the use of the scanners violates the APA, the Religious Freedom Restoration Act (RFRA), the Privacy Act, and the Fourth Amendment.⁸ On May 28, 2010, the TSA's Chief Counsel responded to the petition with a defense of TSA's use of body scanners, addressing several of the claims raised by the EPIC-led coalition.⁹ TSA did not initiate a rulemaking.

⁴ *Id.*

⁵ See, e.g., Thomas Frank, *10 airports install body scanners*, USA TODAY (Jun. 6, 2008), available at http://usatoday30.usatoday.com/travel/flights/2008-06-05-bodyscan_N.htm.

⁶ Petition to the Department of Homeland Security Requesting Formal Rulemaking, May 31, 2009, http://epic.org/privacy/body_scanners/EPIC_Body_Scan_DHS_Petition_05_31_09.pdf

⁷ Letter from Acting Administrator Gale D. Rossides, Transportation Security Administration, to Lillie Coney, Electronic Privacy Information Center, Jun. 19, 2009, http://epic.org/privacy/body_scanners/EPIC_Body_Scan_06_19_09_TSA_Letter.pdf

⁸ Petition to the Department of Homeland Security Requesting Stay of Agency Rule, April 21, 2010, http://epic.org/privacy/body_scanners/EPIC_Body_Scan_04_21_10_DHS_Petition.pdf

⁹ Letter from Chief Counsel Francine J. Kerner, Transportation Security Administration, to Marc Rotenberg, Electronic Privacy Information Center, May 28, 2010, http://epic.org/privacy/body_scanners/EPIC_Body_Scan_05_28_10_TSA_Letter.pdf

On July 2, 2010, EPIC and individual plaintiffs Chip Pitts and Bruce Schneier filed a petition for review with the Court of Appeals for the D.C. Circuit asking the court to remedy TSA's failure to act on the 2009 petition, its refusal to process the 2010 petition, and the ongoing requirement that airport checkpoints use body scanners for primary screening.

In *EPIC v. DHS*, the court partially granted the petition for review.¹⁰ While rejecting the petitioners' Privacy Act, RFRA, and Fourth Amendment claims, the court agreed that the APA compels TSA to conduct notice-and-comment rulemaking regarding its use of body scanners. The court remanded the "rule" to the TSA, instructing the agency to "promptly proceed in a manner consistent with [the court's] opinion." This was in July of 2011.

A year after the D.C. Circuit ordered TSA to conduct an APA rulemaking, the agency had taken no action. On July 17, 2012, EPIC filed a petition for a writ of mandamus asking the court to enforce its earlier mandate. The Competitive Enterprise Institute (CEI), joined by former American Airlines CEO Robert Crandall and seven other public interest groups, filed an amicus brief in support of EPIC's petition. In a per curiam order issued on September 25, 2012, the D.C. Circuit denied the petition for a writ of mandamus, but noted that it "expect[s] that the NPRM will be published before the end of March 2013."¹¹

Just a few days before the court-imposed deadline, TSA published a notice of proposed rulemaking, proposing to add just two sentences to 49 C.F.R. § 1540.107 to note that the agency may use "advanced imaging technology," defined as "screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened."¹²

On June 24, 2013, CEI and Robert Crandall filed comments with TSA in the body scanner proceeding.¹³ CEI and Crandall argued that TSA's proposed rule falls far short of what the APA requires, as it does not give passengers fair notice of their airport screening obligations, and that the agency has failed to justify its proposed rule on risk-based, cost-benefit grounds. Then, once again, the agency stopped moving forward.

¹⁰ *Electronic Privacy Information Center et al. v. Department of Homeland Security et al.*, 653 F.3d 1 (D.C. Cir. 2011).

¹¹ *In re Electronic Privacy Information Center*, No. 12-1307 (D.C. Cir. Sep. 25, 2012) (per curiam).

¹² *Passenger Screening Using Advanced Imaging Technology, Notice of Proposed Rulemaking*, 78 Fed. Reg. 18,287, Docket No. TSA-2013-0004 (Mar. 26, 2013).

¹³ *Comments of the Competitive Enterprise Institute in the Matter of Passenger Screening Using Advanced Imaging Technology, Notice of Proposed Rulemaking*, 78 Fed. Reg. 18,287, Docket No. TSA-2013-0004 (Mar. 26, 2013), available at <https://www.regulations.gov/document?D=TSA-2013-0004-4239>.

On July 15, 2015, more than two years after the closing of the comment period and four years to the day since the D.C. Circuit had ordered the TSA to produce a rule on body scanners, CEI, National Center for Transgender Equality, the Rutherford Institute, and CEI employees Lawson Bader and Marc Scribner filed a petition for writ of mandamus asking the D.C. Circuit to enforce its 2011 mandate and order the TSA to produce a final rule within 90 days. The D.C. Circuit ordered on October 23 that the TSA produce “a schedule for the expeditious issuance of a final rule within a reasonable time.”¹⁴

On March 3, 2016, the TSA finally published its final rule in the *Federal Register*.¹⁵ This was nearly seven years after the original petition for rulemaking.

Is a Prominent TSA “Innovation” Killing American Travelers?

On May 2, 2016, CEI, The Rutherford Institute, and CEI employees Iain Murray and Marc Scribner filed a petition for review of the final rule in the D.C. Circuit. In their opening brief, CEI et al. argued that TSA’s rulemaking illegally failed to consider potential air/road modal substitution due to passengers being turned off by TSA’s intrusive body scanners. Given that road transport is far more dangerous than commercial air travel, some number of people who opt to drive rather than fly inevitably wind up dying in car accidents or killing others.

Cornell University economists Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon have published two studies on the impact of 9/11 and post-9/11 security procedures on the demand for air travel and modal choice. One finding of their research was that for every 1 million decline in airline passenger enplanements, fifteen additional highway fatalities were generated.¹⁶ While TSA failed to do any analysis of the modal substitution question, CEI used the comment record of the proposed rule to extrapolate a rough national modal substitution effect. Based on CEI’s review of the record, approximately 1.5 percent of commenters (1.47854 percent) explicitly stated they have driven or plan to drive rather than fly in order to avoid the indignities of TSA’s AIT-based primary screening.

According to the Bureau of Transportation Statistics, there were 816,763,000 scheduled passenger enplanements in the year ending June 2016, the most recent available data at the time.¹⁷ Assuming TSA’s use of AIT led to a reduction in enplanements of 1.47854 percent, this means 829,020,398 enplanements would have taken place in the absence of the objectionable AIT machines, a difference of 12,257,398 enplanements. If a reduction of one million enplanements leads to 15 additional highway fatalities, modal substitution arising from public opposition to AIT machines can be said to cause 184 additional annual road deaths.

¹⁴ Order, *In re Competitive Enterprise Institute*, No. 15-1224 (D.C. Cir. Oct. 23, 2015) (per curiam).

¹⁵ Passenger Screening Using Advanced Imaging Technology, *Final Rule*, 81 Fed. Reg. 11,363 (Mar. 3, 2016).

¹⁶ Blalock, Garrick, Vrinda Kadiyali, and Daniel H. Simon, *The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel*, 50 J.L. & Econ. 731 (2007).

¹⁷ Bureau of Transportation Statistics, *U.S. Air Carrier Traffic Statistics*, <https://www.transtats.bts.gov/TRAFFIC/>.

In contrast, TSA's break-even analysis assumes the machines would be cost-effective if they save between 20 and 21 lives per year under a variety of scenarios. This means that even if the approximately 1.5 percent modal substitution figure was overestimated by a factor of eight, the additional modal substitution road fatalities would still exceed the life-saving estimates contained in TSA's break-even analysis.

TSA policies may be killing far more people than the agency claims it must save in order to justify the AIT machines. TSA should properly account for the potential deadly impact of body scanners, as we believe it is required to do under the Administrative Procedure Act. The court has yet to rule.

TSA's Unresponsiveness to Federal Declassification Procedure

Giving at least a nod to risk management, TSA in 2013 cited a "risk reduction analysis" in the preamble to the proposed body scanning rule. It purports to show that "the chance of a successful terrorist attack on aviation targets generally decreases as TSA deploys AIT."¹⁸ The relevant question, of course, is not whether an activity reduces risks of attack—many things will—but whether the activity does so in a cost-effective way.

There is no way to tell if the analysis finds this because the TSA classified the document. Classification of the "risk reduction analysis" deprives the public of the benefits that notice-and-comment rulemaking is intended to provide, it deprives the agency of information and data that could improve the rule, and its likely result is more American highway deaths because of a poorly tuned rule.

The TSA should not have declassified the risk reduction analysis. If there are parts that truly merit it, TSA should have left declassified the bulk of the analysis, redacting only specific threat and vulnerability information. Inappropriate use of classification authority has undercut TSA's already very slow and unresponsive rulemaking. TSA also is slow-walking the process for review of its classification decision.

In 2013 and again in 2015, Jim Harper requested mandatory declassification review under Executive Order 13526 of the TSA's "risk reduction analysis." The TSA failed to respond both times. So in November 2016, after passage of more than a year from the last request, he appealed TSA's constructive denial of the review to the Interagency Security Classification Appeals Board (ISCAP). The ISCAP reviews classification decisions to ensure their consistency with federal classification policy.

¹⁸ Passenger Screening Using Advanced Imaging Technology, *Notice of Proposed Rulemaking*, 78 Fed. Reg. 18,287, Docket No. TSA-2013-0004 (Mar. 26, 2013).

The ISCAP requested a copy of the risk-reduction analysis shortly after the appeal was lodged in November 2016. As of April 7, 2017, the TSA has yet to forward the document to ISCAP for its review. In parallel to the drawn out rulemaking process, the TSA is stonewalling the federal government’s classification experts who might review its decision.

What’s More Important? Innovation? Or Legally-Required Consideration?

TSA should not focus on “innovations” that have only arguable security or efficiency benefits and unknown costs to the taxpayer. Rather, if the agency continues to exist at all, it should be brought under control of our nation’s laws, policies, and rational decision-making processes.

Your committee and the courts should make clear that TSA must follow the Administrative Procedure Act before it rolls out new policies. TSA must use risk management and cost-benefit analysis to consider whether policies will be instituted. And these processes must be fully aired—not classified—so that they elicit the knowledge and opinion of the public, including top security and transportation experts.

We are concerned by reports that TSA and other Department of Homeland Security components may be “fast-tracking” the use of technologies such as facial recognition.¹⁹ Such technologies must navigate a Scylla and Charybdis if they are to actually serve the American people and the air transportation industry well. The TSA cannot navigate that path if it does not adhere to the law and good decision-making processes.

On the one hand, there is a high likelihood that facial recognition systems will not work. Due to the vagaries of light, motion, hairstyle, attire, and so on, deployments of facial recognition outside of controlled environments will almost certainly perform more poorly than they do in tests. This means a high likelihood of both false-positive and false-negative errors. False positives would wrongly identify innocent travelers as people who allegedly present some risk to air transportation. The actions that ensue may violate various constitutional rights of travelers and the unenumerated right to travel.²⁰ False negatives would allow allegedly dangerous persons passage through airports unidentified.

On the other hand, if facial recognition systems do work well, they threaten the privacy of millions of law-abiding travelers. Ordinary Americans do not deserve to be identified by automated government surveillance systems, and many more will undoubtedly reject air travel if it is conditioned on their being subjected to such systems.

¹⁹ See, e.g., Russel Brandom, Facial Recognition is Coming to U.S. Airports, Fast-Tracked by Trump, The Verge (Apr. 18, 2017), available at <http://www.theverge.com/2017/4/18/15332742/us-border-biometric-exit-facial-recognition-scanning-homeland-security>.

²⁰ Kent v. Dulles, 357 U.S. 116, 125 (1958); Eunique v. Powell, 302 F. 3d 971, 973 (9th Cir. 2002)(“It is undoubtedly true that there is a constitutional right to international travel.”).

Facial recognition is itself an arguable search of persons under the Fourth Amendment. Facial recognition systems work by converting the features of the face to a matrix of spatial relationships among its features, of colors, and textures. The distances between the eyes, width of the nose, color of the skin, and so on become elements in what is essentially a biometric signature. When the facial signature is collected, there may be no investigation underway, which may seem to imply that there is no Fourth Amendment search—just some inert administrative process. But the conversion of a face image to a facial recognition signature has only one purpose: to find something later.

Searching has two conceptual parts, which usually occur in a particular order. First, the specific thing to be searched for is identified. Next, the field in which it may be found is examined. The search of a wood involves identifying the person, instrumentality, or evidence that may be found there, then marching through the area with eyes peeled for that thing.

Facial recognition reverses these processes. It collects the material to be canvassed—facial signatures—then at any later time canvasses the earlier-collected facial signature data for a match.

The fact that the steps in the process are reversed should not change the conclusion that facial recognition is a search technology and the use of it is a search. Conversion of a facial image to a facial signature that can be scanned for matches is a search of the face itself to render data that make the face amenable to being the object of a later search. It is enough of a step in the process of searching that it is best recognized as a search occurring at the time the processing is done.

Whether facial recognition works or not, the topic raises dozens of policy questions separate and apart from whether or not it is “innovative.” Before facial recognition is deployed, TSA and any other DHS component using it must establish in a public notice-and-comment rulemaking where they propose to use it and during what time periods; what will happen with facial signatures collected, both in terms of comparison to other signatures and in terms of retention; if retained, whether travelers will have access to data collected about them; the security of facial signature data, both in transit and in storage; the opt-out rights of travelers who do not wish to be scanned; and so on.

Conclusion

TSA must not “innovate” on the requirements of U.S. law and sound decision-making. Otherwise, as happened with the “puffer machines,” millions of taxpayer dollars may go to waste on useless technology. If TSA continues in failing to use publicly reviewable risk management and cost-benefit analysis, it will risk yet more taxpayer dollars on machinery that does not provide security-for-value. Just as importantly, if TSA adopts technology because it is innovative and not because it is proven to get the security job done, the agency may drive yet more American travelers away from airports and airlines. Doing so will put them into their cars on the nation’s highways, where they will needlessly die in greater numbers than they do in the very safe air transportation sector.