Privacy Impact Assessment Update
for

TSA Advanced Imaging Technology

January 25, 2011

<u>Contact Point</u>
Robin Kane
Assistant Administrator
Operational Process & Technology
robin.kane@dhs.gov

<u>Reviewing Official</u>
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) is deploying Advanced Imaging Technologies (AIT),[1] including backscatter x-ray and millimeter wave devices, for operational use to detect threat objects carried on persons entering airport sterile areas.[2] AIT creates an image of the full body that highlights objects that are on the body. To mitigate the privacy risk associated with creating an image of the individual's body, TSA isolates the TSA officer (the image operator) viewing the image from the TSA officer interacting with the individual. TSA does not store any personally identifiable information from AIT screening. A PIA on the pilot was published on January 2, 2008, updated on October 17, 2008 and updated again on July 23, 2009 as program developments warranted.

TSA plans to test, and implement as appropriate, Automatic Target Recognition software for AIT machines that display anomalies on a generic figure, as opposed to displaying the image of a specific individual's body. Since the technology uses a generic image that provides greater privacy protections for the individual being screened, systems using Automatic Target Recognition will not isolate the operator viewing the image from the individual being screened. Individuals will continue to be given the option of undergoing a physical screening as an alternative to AIT screening.

Reason for this Update

TSA is updating the AIT PIA for the following reasons: (1) TSA will test Automatic Target Recognition (ATR) software to determine whether it can replace the existing image viewed by the image operator with a generic image on which the location of anomalies are marked; (2) AIT technology has moved from a pilot to normal screening operations; (3) TSA will not use the red/green light signal described in the PIAs dated July 23, 2009 or January 2, 2008 but will instead rely on existing radio communications; (4) the x-ray technologies penetrate the skin sufficiently in some instances to reveal matter that lies adjacent to but beneath the surface of the skin (for example, shin bones); and (5) to reflect the name change to AIT. This PIA update addresses AIT operations for systems equipped both with and without ATR software. Operational differences between systems with and without ATR will be expressly noted. No changes have been made to the operating protocols relevant to the privacy impacts except that ATR-equipped machines will not separate the image operator from the individual being screened.

[1] Previously identified as "Whole Body Imaging."

[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.

Introduction

The Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, makes TSA responsible for security in all modes of transportation, and requires that TSA assess threats to transportation, enforce security-related regulations and requirements, and ensure the adequacy of security measures at airports and other transportation facilities. TSA uses x-ray backscatter and millimeter wave technology in airports to quickly, and without physical contact, screen passengers during primary or secondary screening for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. In the event a suspicious item cannot be cleared visually, the individual will undergo physical screening. TSA used AIT technologies in pilot efforts in both primary and secondary modes at a variety of airports and has moved the technology into normal screening operations.

TSA currently uses two types of AIT technologies: general use backscatter and millimeter wave.

- General use backscatter technology relies on x-ray beams scanned over the body's surface at high speed that are reflected back from the body and other objects placed or carried on the body, where it is converted into a computer image of the subject and displayed on a monitor.[3] The system delivers an extremely low dose of ionizing radiation to the individual and is well within American National Standards Institute (ANSI) standards.[4] For comparison purposes, the x-ray dose received from the backscatter system in use is less than the radiation received in two minutes of airplane flight at altitude.[5] X-rays may in some cases reveal matter underneath and near the surface of the skin (for example, the bones of the shin or forehead). It may also be possible that some medical implants adjacent to the skin will show as an anomaly in the x-ray technologies.
- Millimeter wave technology uses non-ionizing radio frequency energy in the millimeter wave spectrum to generate an image based on the energy reflected from the body. The three-dimensional image of the body is displayed on a monitor[6] for analysis. The energy projected by the system is a fraction of the energy projected by other commercially approved radio frequency devices.

Further safety information can be found on the TSA website.[7]

[3] The monitor will be remotely located for systems not equipped with ATR software, and co-located for systems with ATR software.

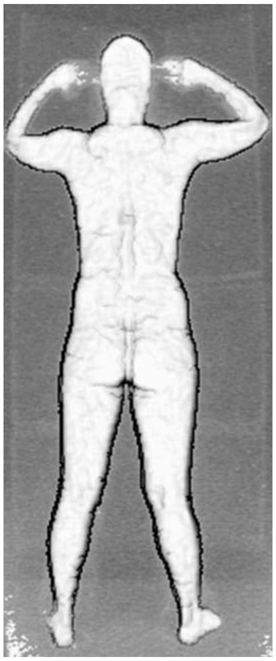
[4] ANSI N43.17-2009

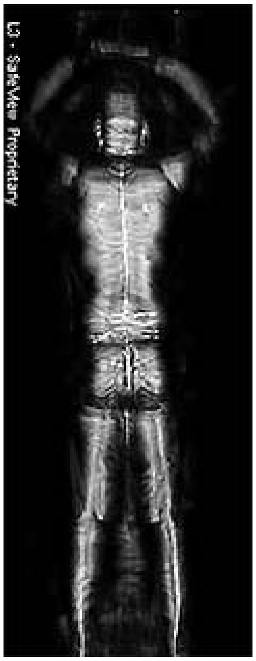
[5] See e.g., FDA notation at: http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm#2

[6] The monitor will be remotely located for systems not equipped with ATR software, and co-located for systems with ATR software.

[7] http://www.tsa.gov/approach/tech/ait/safety.shtm and in the electronic reading room at http://www.tsa.gov/research/reading/index.shtm.

The images created by the AIT technologies are not equivalent to photography and do not present sufficient details that the image could be used for personal identification. Examples of the current level of image detail created by the AIT technology appear below.



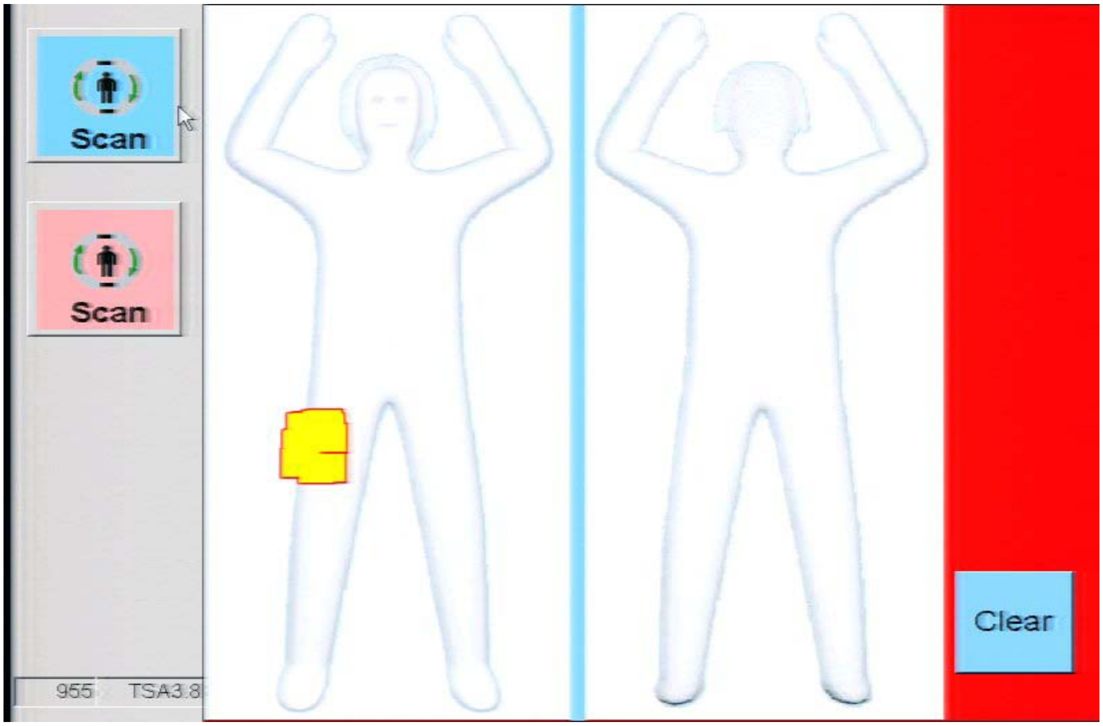


Backscatter image **Millimeter wave image**

Automated Target Recognition

ATR software seeks to replace the current image of the human body with a method for targeting anomalies and highlighting their location on a generic figure. The use of ATR software will reduce the impact to individual privacy by eliminating the image of each individual's body that is generated by the millimeter wave and x-ray technologies, while still allowing appropriate recognition of anomalies. Systems using ATR eliminate the need for a remote image operator, given that the ATR technology allows for the screen with the ATR image to be located within the same vicinity of the officer assisting the screened individual.

A sample image from a system using ATR appears below:



Storage of images

The ability to store images is not included in the software on AIT devices placed in airports, and there is no capability to activate image storage functions by anyone at the airport.[8] Images are maintained on the monitor only for as long as it takes to resolve any anomalies. If the image operator sees a suspicious area or prohibited item, the image remains on the monitor until

[8] 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.

the item is cleared, either when the image operator recognizes the item on the monitor, or by a physical screening that is completed by a screening officer located with the individual undergoing screening. The AIT equipment does not retain the image. In addition, image operators are prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras. For AIT machines not equipped with ATR software, the image operator is located remotely from the individual being screened and is not able to see the individual.

<u>What to expect</u>

At locations using AIT that are not equipped with ATR, TSA will post signs showing an image for the type of AIT being used (x-ray or millimeter wave) and informing that individuals may decline AIT in favor of physical screening. Anonymity is preserved by physically separating the image operator from the individual undergoing screening, and by algorithms that either blur or degrade the image of the face of the individual. The officer that is stationed with the individual does not see the AIT image.

At locations piloting AIT with ATR software, TSA will post signs showing a sample ATR image and informing individuals that they may decline AIT in favor of physical screening. Because the ATR software replaces the individual's image with that of a generic figure, the image screen will be co-located with the individual being screened and there will not be a remotely-located image operator. The TSO at the AIT will view both the individual and the ATR image. If an anomaly is identified, the physical screening will target the location of the anomaly. If there are multiple anomalies, the individual may receive a full screening.

Rules governing the use of AIT machines are documented in standard operating procedures (SOP), and compliance with these procedures is reviewed on a routine basis. Due to the sensitivity of the technical and operational details, the SOP will not be publicized; however, TSA's Transportation Security Officers (TSOs) receive extensive training prior to operating AIT technology.

The AIT program recognizes and seeks to accomplish the twin goals of minimizing privacy intrusions, while ensuring that prohibited items, such as weapons and explosives, do not enter the airport's sterile area. The AIT systems present images of potential threats while minimizing individually identifying features.

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 extensive information on AIT technologies on its website (www.TSA.gov), including a PIA in January 2008 and related updates thereafter, and conducted outreach with national press and with privacy advocacy groups to explain the evaluation of AIT technologies. Signage regarding the program will be made available at each AIT site that will show the AIT image in use at that location. While most PIAs are conducted on IT systems that collect and retain PII, TSA has configured the AIT technologies it is using such that it does not retain the images once the individual has been screened. TSA is conducting this PIA to update its efforts to provide transparency and notice to the public regarding TSA's use of AIT technologies.

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 primary screening using AIT will have the option to decline an AIT screening in favor of physical screening. Individual participation and consent is exercised by the individual's selection of the screening method and no individual is required to use AIT for screening. Further notice is provided by the availability of signage that explains the technology and shows a sample image.

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. 49 U.S.C. § 114(d). 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. 49 U.S.C. § 44912 note. AIT technologies are being used to identify prohibited items, particularly non-metallic threat objects and liquids secreted on the body. An image appears on the AIT monitor to screen for threat objects and is cleared from the screen as soon as any anomalies are resolved. Images are not stored. The image is not connected to an individual identity and is not sufficiently detailed to identify an individual. ATR software identifies the location of the anomaly on a generic figure. Because of the greater privacy protections provided by a generic figure, AIT machines with ATR will deploy the image monitor near the AIT machine so that the screening officer can view it, and will not use a remote image operator.

4. Principle of 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. TSA does not save the image in connection with the use of AIT technologies. While the technology can be configured to store images, TSA considered the privacy issues of this storage feature and carefully evaluated all potential uses of the images, including for training, investigations, or possible prosecution of persons caught with prohibited items. Based on this evaluation, TSA decided to have the manufacturer produce a software package that does not include data storage capabilities for AIT used in operations. Individual AIT operators do not have the capability to enable image retention. As a result, the image will only be available during the time the individual is being screened and will be cleared from the screen immediately thereafter. Images are not stored.

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 anomalies that may be threat items. Once any anomaly is resolved, the image is cleared from the screen and not stored, 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. For AIT machines not equipped with ATR software, images viewed by image operators are not shared with the screening officer.

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 AIT images are generated by direct contemporaneous observation. Accordingly, it 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. The images are not retained, thereby further mitigating any data quality or integrity issues.

Viewing of AIT images occasionally requires interpretation of the images. An AIT image with an anomaly that may represent a prohibited item will require physical screening of the traveler before they may proceed into 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 between the checkpoint and the viewer by a landline connection; and cannot be lost, modified, or disclosed. In addition to physical security from a landline connection, the data transmitted through the landline is encrypted (for Backscatter) or is transmitted in a proprietary format that cannot be deciphered without the proprietary technology (for Millimeter wave). TSA's decision not to retain images mitigates further data storage security issues. In addition, the computers used to process and present the images will be locked with both physical and software controls to prevent the insertion of any storage media or other communication devices. For AIT machines not equipped with ATR software, administrative controls limit access to the remote image viewing rooms and prohibit TSOs from bringing photographic devices, including cell phone cameras, into the room in which images are viewed. Appropriate discipline, including termination, may be imposed for violation of the protocols.

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.

TSOs operating AIT technology are given extensive training both in detecting threat items as revealed by the AIT technology, and the operational protocols that protect the privacy of individuals undergoing AIT screening. Specifically, TSOs will undergo privacy and Privacy Act training developed by the DHS Privacy Office for the Department. Supervisors will ensure that policies and procedures regarding photography are fully enforced. In addition to administrative controls imposed by the operating protocols, technical controls also enforce accountability since AIT technology settings are locked and cannot be changed by anyone at the airport.

9. Additional Issues

Discuss any issues impacting privacy not covered by the eight FIPPs.

There are none.

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. The operating protocols of remote viewing for AIT machines not equipped with ATR software, coupled with no image retention, are strong privacy protections that do not detract from the security benefits that are to be achieved. ATR software provides even greater privacy protections by eliminating the human image that appears with the existing AIT technologies.

Responsible Officials

Robin Kane

Assistant Administrator

Operational Process & Technology

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security