Privacy Impact Assessment
for

TSA Whole Body Imaging

January 2, 2008

Contact Point
Mike Golden
Assistant Administrator
Operational Process & Technology
Mike.Golden@dhs.gov

Reviewing Official
Peter Pietra
Director, Privacy Policy & Compliance
Transportation Security Administration
TSAprivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) will conduct pilot operations to evaluate the use of various Whole Body Imaging (WBI) technologies, including backscatter x-ray and millimeter wave devices, to detect threat objects carried on persons entering airport sterile areas[1]. WBI creates an image of the full body, showing the surface of the skin and revealing objects that are on the body, not in the body. To mitigate the privacy risk associated with creating an image of the individual's body, TSA isolated the Transportation Security Officer (TSO) viewing the image from the TSO interacting with the individual. During the initial phase of the pilot, individuals who must undergo secondary screening will be given the option of undergoing the normal secondary screening technique involving a physical pat down by a TSO or a screening by a WBI device. A subsequent phase will evaluate WBI technology for individuals undergoing primary screening. Individuals will be able to choose to undergo WBI screening in primary.

In the interest of transparency to the public, this Privacy Impact Assessment (PIA) conducted pursuant to Section 222 of the Homeland Security Act ensures that technologies sustain and do not erode privacy protections. TSA has developed operating processes for the WBI, used for pilot operations, that do not collect, store, or distribute any personally identifiable information.

Introduction

The Aviation and Transportation Security Act (ATSA), PL 107-71, directs 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." Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA proposes to evaluate the effectiveness of WBI technologies in operational settings. TSA tested WBI technologies in a controlled laboratory setting and determined the technologies to be technically functional. In the operational setting, TSA will determine whether sufficient passenger throughput can be achieved while maintaining threat detection levels, and will compare operational detection levels between technologies.[2] TSA will use x-ray backscatter and millimeter wave technology in a limited

---

[1] "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.

[2] TSA additionally requested that the National Research Council study "technologies to protect the nation's air transportation system from attacks by terrorists and others of like mind." The study, *Assessment of Millimeter-wave and Terahertz Technology for Detection and Identification of Concealed Explosive and Weapons*, published in 2007, provides further discussion of the systems, their technologies, and a proposed implementation strategy for their deployment.
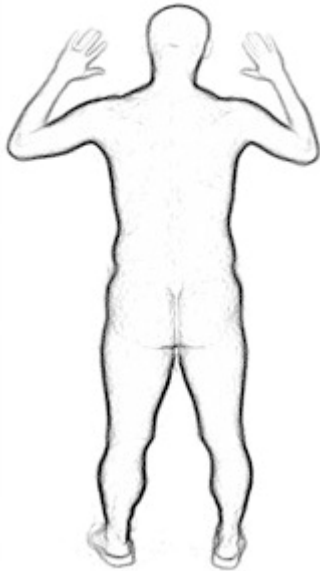
number of airports. By using passenger imaging technology, TSA expects to be able to quickly, and without physical contact, screen passengers during primary or secondary inspection for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. In the event a suspicious item cannot be cleared visually, the individual will undergo a physical pat down targeted to locations identified through the WBI visual inspection.

TSA will test two types of WBI technologies: backscatter and millimeter wave.

- Backscatter technology relies on a narrow, low intensity x-ray beam scanned over the body's surface at high speed that is 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 remote monitor. For comparison purposes, the x-ray dose received from the backscatter system is equivalent to the radiation received in two minutes of airplane flight at altitude (.02 millirem for two scans by backscatter compared to .0276 millirem for two minutes of a flight).

- 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 remote monitor for analysis. The energy projected by the system is 100,000 times less than a cell phone transmission (.00000597 mW/cm^2 for millimeter wave technology compared to 37.5 mW/cm^2 for a cellphone).

The images created by the WBI technologies are not equivalent to photography and do not present sufficient details that the image could be used for personal identification. Below are examples of the current level of image detail created by the WBI technology, which may change. Sample images will be made available to individuals at the location of the WBI equipment to show the image to individuals deciding whether or not to choose the WBI visual inspection instead of the physical pat down inspection. It should be noted that the millimeter wave image rotates and a blur appears over the face as the front appears in view.

Backscatter image   **Millimeter wave image**

While the equipment has the capability of collecting and storing an image, the image storage functions will be disabled by the manufacturer before the devices are placed in an airport and will not have the capability to be activated by operators. Images will be maintained on the screen only for as long as it takes to resolve any anomalies; if a TSO sees a suspicious area or prohibited item, the image will remain on the screen until the item is cleared either by the TSO recognizing the item on the screen, or by a physical screening by the TSO with the individual. The image is deleted in order to permit the next individual to be screened. The equipment does not retain the image. In addition, TSOs will be prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras. Rules governing the operating procedures of TSOs using this WBI equipment are documented in standard operating procedures (SOP), and compliance with these procedures is reviewed on a routine basis. Due the sensitivity of the technical and operational details, the SOP will not be publicized, however, TSOs receive extensive training prior to operating WBI technology.

The TSO who views the image will be located remotely from the individual being screened so the TSO will not be able to see the actual individual. The TSO viewing the image will communicate with the TSO at the checkpoint through a red/green light system. If there is a red light, the TSO will communicate via radio to direct the TSO at the checkpoint to the location on the individual's body where a threat item is suspected. The TSO at the checkpoint will then conduct a physical pat-down that is focused on the particular area and not necessarily of the

individual's entire body which would normally occur absent the added information from the WBI technology.

The WBI pilot 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 WBI system present images of potential threats while minimizing individually identifying features. Further, the operational documentation cites with approval NRC Publication NMAB-482-1, *Airline Passenger Security Screening: New Technologies and Implementation Issues*, (1996), and appears to have considered carefully the issues raised in that publication.

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. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as 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, which 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 WBI technologies on its website (www.TSA.gov) beginning in February 2007, and conducted outreach with national press and with privacy advocacy groups to explain the evaluation of WBI technologies. Informational brochures regarding the program will be made available at each WBI site that will show a WBI image that the technology will create. Most PIAs are conducted on IT systems that collect and

Homeland Security

retain PII. TSA has configured the WBI technologies it is using such that they do not retain the images once the individual has been screened. TSA is conducting this PIA in order to be transparent and provide notice to the public regarding TSA's use of WBI 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 will have the option to select a WBI screening. Individuals referred to secondary inspection are offered the option to undergo WBI screening as an alternative to the pat-down screening that would otherwise be required. Individual participation and consent is exercised by the individual's selection of the screening method and no individual is required to use WBI for screening. Consent is informed by the availability of brochures that explain the technology and show 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 USC §114. 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 USC §137.

Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA is evaluating the use of WBI as an improvement over current threat item detection by metal detector and pat-down, particularly with respect to non-metallic threat objects and liquids. An image will appear on the WBI viewer to screen for threat objects and will be deleted as soon as any anomalies are resolved. The image is not connected to an individual identity and is not sufficiently detailed to identify an individual.

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).

WBI technologies identify objects on the outside of the physical body and do not reveal implants beneath the surface of the skin. TSA does not save the image in connection with the use of WBI 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 for training, investigations, or possible prosecution of persons caught with prohibited items. Based on this evaluation, TSA decided to have the manufacturer disable the data storage capabilities prior to delivery to TSA. Individual operators do not have the capability to reverse 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 deleted immediately thereafter.

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.

TSOs sitting in the remote viewing room are the only persons to see the WBI images that appear on the screen transiently for the purpose of identifying any potential threat items. The TSOs at the screening location and the supervisory TSO overseeing their actions are prohibited from entering the remote room and viewing the images on the screen. Once any anomaly is resolved, the image is deleted, and therefore cannot be used for any other purpose or shared with anyone. The images will not be used in any other context inside DHS and will not be shared 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 WBI images are generated by direct observation by the imaging technology. 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 pat down 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 WBI images occasionally requires interpretation of the images. A WBI image with a suspicious area (one in which it is unclear whether there is a prohibited item) will require additional screening of the traveler with a limited pat-down, focusing on the suspicious area alone. The traveler may be patted down in the screening area, an alternate screening area, or in a private 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.

WBI data is transmitted between the checkpoint and the viewer by a landline connection and cannot be lost, modified, or disclosed. Backscatter images are encrypted. Millimeter wave data is transmitted in a proprietary format that cannot be deciphered without the proprietary technology. 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. Administrative controls limit access to the remote viewing rooms to TSOs and prohibit TSOs from bringing photographic devices, to include cell phone cameras, into the room in which images are viewed.

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 WBI technology are given extensive training both in detecting threat items as revealed by the WBI technology and the operational protocols that protect the privacy of individuals undergoing WBI 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 WBI technology settings are locked and cannot be changed by the TSO operating the equipment.

9. Additional Issues

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

There are none.

Conclusion

WBI technology used in the pilot program has the potential to improve threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical pat-down is uncomfortable. The operating protocols of remote viewing and no image retention are strong privacy protections that permit security benefits to be achieved. TSA will update this PIA as needed if there is a decision to utilize one or both of these WBI technologies beyond pilot operations in several airports.

Responsible Officials

Mike Golden

Assistant Administrator

Operational Process & Technology

Approval Signature Page

<u>Original signed and on file with the DHS Privacy Office</u>

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security