Privacy Impact Assessment
for

Stand-Off Detection (SPO)

December 23, 2008

Contact Point
Robert Pryor
Manager, Surface Protection Technology
TSA Office of Security Technology
Robert.Pryor@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 deploy advanced explosives detection technology using passive millimeter wave (PMMW) screening technologies as part of the agency's efforts to ensure the safety of travelers. The objective is to identify individuals who may seek to detonate explosives in transportation facilities. This Privacy Impact Assessment is being conducted to provide transparency into TSA operations affecting the public.

Introduction

TSA has broad statutory responsibility and authority for ensuring the security of all modes of transportation, including, among others, civil aviation, ferries, passenger rail, and mass transit. 49 U.S.C. § 114(d). That authority includes the development and use of new technologies in all of those environments. 49 U.S.C. § 114(f). Pursuant to these authorities, as well as its general authorities to conduct research and development to enhance transportation security, TSA will deploy advanced standoff explosives detection capabilities in the form of PMMW technologies as part of the agency's efforts to ensure the safety of travelers in transportation settings. Figures 1 and 2 below depict the two models in use by TSA, the SPO-7 and SPO-20.[1]

Figure 1 - SPO-7

Figure 2 - SPO-20

Passive imaging detection techniques rely on collecting naturally occurring radiation and using the contrast between apparently "warmer" and "colder" objects, which usually results from contrasts between the different materials' ability to absorb and radiate energy. Each SPO unit

[1] Currently there are two SPO models available for use in the United States, the SPO-20 and the SPO-7R. Both the SPO-20 and SPO-7R systems perform and operate exactly the same manner – their differences are related to their size and range. The SPO-20 is the larger of the two systems and has a greater range. The SPO-7R system is smaller and more mobile system with a shorter range.

consists of two separate sensors and a monitoring location. Sensors receive PMMW to detect the presence of an anomaly which could be indicative of an explosive device. The SPO operator may engage other TSA or law enforcement personnel to address any anomaly.

A closed circuit television (CCTV) image is provided to the operator to allow precise remote alignment of the receiver on the individual being scanned. The images displayed on the SPO monitor are the same as images viewed by the naked eye and are the only personally identifiable information collected.

Using SPO, TSA expects to be able to quickly, and without physical contact, screen individuals for items hidden under layers of clothing, which could indicate the presence of an explosive device. Individuals will not be asked to stand in place, nor will they need to break stride during the use of the sensor. As noted above, the Transportation Security Officer (TSO) at the monitoring location will see the same images as viewed by the naked eye. There is no X-ray or other penetration of garments and no collection of identifiable information or display of bodily characteristics.

Figure 3 - The TSO will see the same images as viewed by the naked eye

SPO technology is expected to be used in any transportation mode to assist in preventing disruptions to transportation and promote transportation security.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 sets forth 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 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.

In addition to the technology itself, which is large and obvious to approaching individuals and is manned by personnel during operation, notice will be provided through prominently displayed signage. TSA is also providing general notice through this PIA.

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.

Generally, individuals do not have an opportunity to provide consent to the collection of images by the SPO technology. TSA provides notice to individuals through prominently displayed signage that the technology is being used and individuals may choose to decline to enter the area where SPO operations are taking place.

TSA does not anticipate retaining the images of most individuals screened by the SPO. Subject to existing SOPs related to an incident, TSA may retain images of those individuals on whom the SPO detects an anomaly indicative of a potential explosive device. Individuals may request access to information that may have been retained pursuant to the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 CFR Section 5.21 by submitting a Freedom of Information Act / Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, West Tower
FOIA Division

601 South 12th Street
Arlington, VA 22202-4220

FOIA / PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (http://www.tsa.gov/public/contactus). The FOIA / PA request must contain the following information: Full name, current address, date and place of birth, telephone number, and email address (optional). Privacy Act requesters must either provide a notarized and signed request or sign the request pursuant to penalty of perjury, 28 U.S.C. § 1746. Please refer to the TSA FOIA web site (http://www.tsa.gov/public).

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. 49 U.S.C. § 114. TSA is authorized to "assess threats to transportation," and "identify and undertake research and development activities necessary to enhance transportation security." 49 U.S.C. § 114(f). 49 U.S.C. § 44912(a)(1) directs TSA to "establish and carry out a program to accelerate and expand the research, development, and implementation of technologies and procedures to counteract terrorist acts against civil aviation." To develop the focus and priorities of the program, the Administrator must periodically review threats to civil aviation, including the disruption of civil aviation service and the potential release of chemical, biological, or similar weapons or devices either within an aircraft or an airport. 49 U.S.C. § 44912(b).

Pursuant its authorities, TSA is deploying SPO technologies to help mitigate the threat of a terrorist attack in the lobby or other public areas connected with public transportation.

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).

As described in the introduction, the unit consists of two separate sensors and a monitoring location. The SPO detects potential explosives hidden under individuals' clothing. On the screen, it produces a green-to-red scale that suggests the presence of anomalies such as explosives.

The human images are the same images as viewed by the naked eye and do not contain any associated personally identifiable information. When there is no indication of an anomaly,

the image of the individual is not saved. When there is an indication of an anomaly, TSA will temporarily retain the image of the individual until the anomaly is resolved. In some instances TSA may share the image with law enforcement and transportation facility operators if it is necessary to locate an individual who has moved out of the area before there has been an opportunity to resolve the anomaly. If the potential threat is resolved, the image will be deleted by the end of the operational shift.

If an item is discovered and an incident report is generated, the image may be appended to the incident report and retained. These records are covered by TSA's Privacy Act system of records, DHS/TSA 001 Transportation Security Enforcement Records System (TSERS). In addition, the image may be provided to local law enforcement for their law enforcement report. After the image is appended to the incident report, it will be deleted from the SPO.

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.

The human images displayed on the SPO monitor are the same as images viewed by the naked eye; there is no X-ray or other penetration of garments and no generation of images or display of bodily characteristics. Images temporarily stored on the SPO will not have additional personally identifiable information stored with them. Once an anomaly is resolved, the image is deleted from the SPO, and therefore cannot be used for any other purpose or shared with anyone.

TSA may share images of those individuals for whom the SPO indicates the potential presence of a threat with law enforcement for purposes of resolution. The sharing is compatible with the purpose of the original collection.

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 SPO images are similar to CCTV or other camera images. Accordingly, these images are accurate, timely, and complete, and are directly relevant to the detecting the presence of an anomaly indicative of an explosive device.

A CCTV image is provided to the operator to allow precise remote alignment of the receiver on the individual being scanned.

The minimal privacy risk associated with this technology is the retention of the image of an individual, which does not contain any other kind of PII. The privacy risk is minimal because

TSA only retains SPO images under a limited set of circumstances as discussed in Sections 2 and 4. All other images are either not retained or are deleted at the end of the shift.

SPO does not collect additional personally identifiable information (such as name); thus individuals remain anonymous to TSA unless the interaction leads to an incident report.

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.

TSA will secure SPO images against unauthorized use through a layered security approach involving procedural and information security safeguards. While the data is on the SPO, the data will be encrypted using National Institute of Science and Technology (NIST) standards and industry best practices. These standards will also be applied if data is transferred from the SPO to the TSA incident reporting system. Only TSA employees with proper security credentials and passwords, and a need to know to fulfill their duties, will have access to the SPO and SPO images. Access to SPO images is limited to authorized individuals with a need-to-know.

To the extent possible SPO monitors will be positioned to limit the public's ability to view images. To further restrict the ability of unauthorized individuals to view images on the monitor TSA has installed polarizing filters which limit the field of view to the TSA operator.

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.

TSA personnel operating SPO technology are given training in systems operation protocols and processes for protecting the privacy of individuals undergoing SPO screening. Further, TSA personnel undergo Privacy Act training within 30 days of employment.

9. Additional Issues

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

None

Conclusion

SPO technology is designed to search for anomalies that may indicate the presence of explosives concealed on an individual's body. The visual image seen by the SPO operator is no different than what is visible to anyone seeing the individual, with only a red-green indicator bar on the side of the screen indicating relative anomalies.

Responsible Officials

Robert Pryor
Manager, Surface Protection Technology
TSA Office of Security Technology
Robert.Pryor@dhs.gov

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security