Privacy Impact Assessment Update
for the

Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests

DHS/S&T STIDP/PIA-008(b)

December 17, 2012

Contact Point
Patricia Wolfhope
Human Factors Division
Science and Technology Directorate
202-254-5790

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
202-343-1717

Abstract

The Department of Homeland Security Science and Technology Directorate (DHS S&T) Human Factors Division is using the Standoff Detection Test Bed to test and evaluate the Biometric Optical Surveillance System (BOSS). BOSS is a facial recognition technology that matches 3D signatures from captured facial images with enrolled images stored in the system database. S&T is conducting this Privacy Impact Assessment (PIA) to address privacy concerns raised by testing the facial recognition technology.

Introduction

As part of the expanded use of the Standoff Detection Test Bed, as documented in the Standoff Technology Integration and Demonstration Program (STIDP) PIA, S&T Human Factors Division will use the test bed to test and evaluate the BOSS facial recognition technology. The BOSS technology consists of two cameras capable of taking stereoscopic images of a face and the back end Remote Matching System (RMS). Stereoscopic images are two images of the same object, taken at slightly different angles that create an illusion of 3-dimensional depth from the 2-dimensional images. The cameras transfer the pair of images to the RMS via fiber optic or wireless technology. The RMS then processes and stores the two images into a 3D signature, which is the mathematical representation of the stereo-pair images that the system uses for matching. Using the BOSS facial recognition algorithms, the signature is matched against a locally stored database created from volunteers, using a combination of mathematical and statistical analysis.

BOSS is capable of capturing images of an individual at 50-100 meters in distance. The system can capture images of subjects participating from a specific distance, or be set up in a way that tracks and passively captures frontal face images of an individual as he/she moves in front of the camera.

During the testing and evaluation activities, Pacific Northwest National Laboratory (PNNL) and other university researchers capture the facial images of volunteer test subjects in a number of different scenarios according to the test plan, in order to test system capabilities. These scenarios can include a single test subject, multiple test subjects, a single passive test subject, or multiple passive test subjects walking through the test bed. The 3D signatures are matched to the database containing enrollment images of volunteers taken before the testing activity. The PNNL test plan that is used during the events taking place at the Standoff Detection Test Bed incorporates both types of subjects—those that actively look at the camera and passive subjects that walk in the camera's range. Testing with subjects who actively look at the camera establishes a baseline performance of the system for each testing activity and subject testing of

individuals who walk in the camera's range determines the performance of the system in a quasi-operational environment.

All volunteers sign informed consent forms prior to the data collection. No additional information is collected from the volunteers, and PNNL does not link any identifying information to the individual's images. The objective of the test is to match the captured images taken of the volunteers with the enrollment images stored in the database. Because testing is being conducted at a public venue, members of the public may be present during the tests, and their images may incidentally be captured as they walk past the cameras. However, those images are not recorded, stored, or matched to the database. Additionally, notice is posted to inform the public of these tests. An alternative route is provided so they can avoid the testing area.

PNNL works with a local 6,000-seat venue (the Toyota Center located in Kennewick, Washington) to serve as a long-term testbed for the project. Since 2008, the use of the Toyota Center involved integrating and conducting tests on technologies developed or acquired by PNNL under contract to support the STIDP test objectives. The Toyota center provides representative crowd dynamics using a relatively small venue with a simple footprint.

This project includes the creation of a gallery of enrolled signatures that are stored in the BOSS database. Currently, there is no large-scale repository of facial images that DHS is collecting specifically for facial recognition. The majority of facial images available to federal, state, and local law enforcement, and first responders are collected at border crossings by Customs and Border Protection or mug shots collected upon arrest. These single, frontal images collected during operations are not well-suited for stereoscopic facial recognition matching by BOSS. However, DHS recognizes the potential capability to match images of faces to these existing legacy databases and thus directed S&T to perform facial recognition on a set of better, operationally-relevant data.

These signatures include enrollment images of volunteers, along with images collected from publically available sources, including mug shots published on a Sheriff's Office website. The mug shots do not include any other personal information, such as first and last name, address, and arrest record. This gallery of images is used to populate the BOSS database in order to obtain better statistical relevance during the evaluation of the BOSS capabilities. These images are only being used to expand the size of the BOSS database that the 3D signatures are matched against. A bigger database provides greater statistical relevance and enables the researchers to better examine the margin of error. By matching the 3D signatures across 1000 versus 30 signatures, researchers are better able to guarantee accuracy in the matches. The larger BOSS database mimics legacy DHS end-user data, and the downloaded images are used simply for "background noise."

S&T does not receive any images or data captured during the testing activities; S&T only receives a final report at the conclusion of each test exercise. BOSS is being tested as a

standalone system; it will not be integrated into STIDP. PNNL, performers, and researchers adhere to the privacy mitigations and protections documented in the STIDP PIA, as well as the S&T Research Projects Involving Volunteers PIA[1].

Reason for the PIA Update

The STIDP PIA Update published in October 2010 covers the use of the Standoff Detection Test Bed to test and evaluate various standoff detection and first line sensor technologies. The PIA documents the expanded use of the test bed to test other technologies. S&T is updating the PIA to include the testing and evaluation activities of BOSS at the SDTB site. While BOSS will not be integrated into the STIDP systems, it does raise separate privacy concerns; this PIA update will address the concerns and how S&T mitigates such concerns.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

During the testing and evaluation activities, PNNL researchers collect enrollment images of the volunteer participants that the captured images are then matched against. The volunteers are assigned a subject number that is used for volunteer management and match verification purposes only. No other identifying information is collected from volunteers during the tests. Images of passersby not involved with the tests may incidentally be captured during testing activities. If this occurs, researchers will not record, store, or match the images to the database. If a passerby's image is accidentally captured during testing, that specific test run is aborted, the captured images with passerby are deleted, and the run is repeated.

Researchers also populate the system database with images downloaded from a publically available Sheriff Office website. These images may include mug shots of individuals. Only the images are enrolled into the database; no other personally identifiable information is collected or stored in the database and no effort is made to identify any of the individuals.

Uses of the System and the Information

PNNL researchers only use the images collected to conduct matches in the test setting. This helps PNNL researchers ascertain the technology's effectiveness and accuracy in performing matches. This also allows PNNL to review and evaluate the system's operational

[1] The S&T Volunteers PIA can be found here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_volunteers.pdf

performance and provide recommendations as to what performance measures need to be adjusted or modified. The images are not used for any other purposes. Any images of non-volunteers incidentally captured during the tests will not be used by researchers; no matches will be performed using these images.

Images downloaded from publically available sources are used to create a gallery of legacy, operationally relevant data in the BOSS database. These extra images are used to expand the size of the BOSS database to mimic DHS databases in order to obtain statistical relevance in the study. They effectively create "background noise" in the system and are not intended to match the images of the volunteers.

Retention

PNNL researchers may retain images of volunteers for the duration of the project. At the end of the project the enrolled and captured images are destroyed. Some images of volunteers may be published in reports to demonstrate the technology's capability. No identifying information will be published with the images. All volunteers receive notice prior to data collection on the use and retention of their images. Images that are incidentally captured of passersby are not retained in the BOSS database.

Internal Sharing and Disclosure

PNNL researchers do not share images with any entities outside the research team. S&T does not receive or share any images or personal information; S&T only receives a final report at the conclusion of the tests. Some images of volunteers may be published in reports to demonstrate the technology's capability. No identifying information will be published with the images.

External Sharing and Disclosure

PNNL researchers do not share images with any entities outside the research team. S&T does not receive or share any images or personal information. Some images of volunteers may be published in reports to demonstrate the technology's capability. No identifying information will be published with the images.

Notice

Volunteer participants in the study receive notice and provide informed consent prior to data collection. Furthermore, notice will be posted to notify the public of testing activities and inform passersby of an alternative route if they wish to avoid the testing area. The notice posted will be visible to the public and the alternative route will be clearly marked.

Individual Access, Redress, and Correction

Volunteers receive notice and must provide informed consent prior to participating in the tests. They are able to pull out of the study at any time. If a volunteer decides to remove his or

herself from the activities, his or her data is removed immediately from the system. The purpose of the tests is to test and evaluate the BOSS image matching capability. Any inaccurate matches are still valuable to the research process and are taken into account when making improvements on the system. Volunteers are not impacted by incorrect matches.

Images of passersbys that are incidentally captured are not used and are immediately deleted; therefore it is not possible to access or retrieve them.

Technical Access and Security

BOSS is tested as a standalone system and is not connected to the internet or DHS network. Access controls are in place to ensure that only authorized researchers have access to the system and the images. The system is also encrypted to prevent unauthorized use of the images.

Technology

The BOSS technology will not be integrated into the existing STIDP technology suite. S&T HFD is testing the technology as a standalone system to better understand the limitations of facial recognition using stereoscopic recognition techniques. Current limitations of facial recognition technology, especially on passive subjects, includes matching images of a face with changes in illumination and pose angle at the time of capture, as well as artifacts including glasses, hats, facial hair, etc., against a gallery of previously-enrolled individuals. One characteristic of a good biometric modality is its permanence, which is inherently challenging with images of faces which can change over time (ageing, etc.); change over days (facial hair, glasses, hats, etc.); or change over environments (indoors vs. outdoors, pose angle, etc.). However, the relative uniqueness and collectability of a face, for facial recognition purposes, make it an advantageous technology to develop and implement for national security purposes.

Responsible Official

Patricia Wolfhope
Science and Technology Directorate
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor

Acting Chief Privacy Officer
Department of Homeland Security