Privacy Impact Assessment
for the

Data Collection for the Centralized Hostile Intent Project

DHS/S&T/PIA-029

June 9, 2015

Contact Point
Dr. Kai-Dee Chu
Resilient Systems Division
Science and Technology Directorate
(202) 254-2315

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Centralized Hostile Intent (CHI) program within the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) collects video images of trained actors posing as passengers, as well as members of the traveling public at the Theodore Francis Green Memorial State Airport in Providence, Rhode Island. The Centralized Hostile Intent program goals are to assess whether behavioral indicators of malicious intent can be observed by trained professionals (e.g., TSA Behavior Detection Officers) from video images in a remote environment. Remote screening offers the potential for the Transportation Security Agency (TSA) to expand the scale of its behavior detection program without correspondingly increasing staffing costs. The data collection involves collection of Personally Identifiable Information (PII) in the form of video images that include the face and body of trained actors and members of the traveling public. This Privacy Impact Assessment (PIA) addresses privacy issues associated with the collection of the video data for the Centralized Hostile Intent (CHI) program and updates the previously published PIA for "Project Hostile Intent Technology."

Overview

The Department of Homeland Security (DHS), Science and Technology Directorate (S&T) is responsible for conducting basic and applied research, development, testing, and evaluation activities that are relevant to any or all elements of the Department. S&T is researching the use of video images of trained actors exhibiting behavioral indicators that mimic passengers who exhibit suspicious behaviors with hostile intent attempting to travel within the U.S. transportation infrastructure. The Transportation Security Agency (TSA) currently performs behavior-based risk assessment via the Behavior Detection and Analysis (BDA) program in multiple airports in the United States.[1] The BDA program uses trained professionals, referred to as Behavior Detection Officers (BDO), to perform behavior-based screening. BDOs are trained to identify passengers exemplifying a discrete subset of behavioral indicators to inform risk-based screening decisions. S&T previously conducted a Privacy Impact Assessment (PIA) regarding hostile intent technology in 2008.[2]

Centralized Hostile Intent (CHI) is a research effort by S&T to (1) evaluate whether the behavioral indicators used to screen for passengers with hostile intent can be reliably observed

[1] More information about the BDA (formerly SPOT) program can be found in the DHS/TSA/PIA-016(a) Screening of Passengers by Observation Technique (SPOT) Program, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-spot-update.pdf.

[2] *See* DHS/S&T/PIA-005 Project Hostile Intent Technology (February 25, 2008), *available at* http://www.dhs.gov/privacy-documents-st. "Project Hostile Intent (PHI) is a research effort by the Science and Technology Directorate to ascertain whether screening technology can aid DHS screeners in making better decisions by supplementing the current screening process (wherein a human screener evaluates an individual's behavior) with training and computers. This Privacy Impact Assessment (PIA) addresses privacy impacts of this program, and specifically, the temporary storage of video images during field tests of PHI's performance with real behavioral data to ensure that it is effective in a 'real world' environment."

by BDOs via live video images as opposed to in person; (2) explore whether behavior-based screening can be successfully performed in a remote (i.e., centralized) environment; and (3) develop a unique and operationally relevant dataset to research and test automated video analytic solutions for hostile intent detection and tracking. To facilitate this research, S&T is conducting a video data collection at the T.F. Green Airport in Providence, Rhode Island (T.F. Green Airport, PVD). S&T presently does not have the capability to assess whether behavioral indicators can be reliably observed from video images in a test environment. Therefore, S&T is conducting a video image collection in an operational environment.

The video data collection will collect Personally Identifiable Information (PII) in the form of facial images and anthropomorphic data. S&T will collect PII from trained (volunteer) actors posing as passengers and may incidentally collect PII from members of the traveling public and airport personnel who may be near them. S&T will collect video images at designated areas throughout the airport, including a TSA security checkpoint, ticket counter, baggage claim, and airport entrance. The trained actors role-play a series of different scenarios (i.e., vignettes) that are video recorded. No audio or conversations are recorded at any time. During video collection and when feasible, collection sites are cordoned off and physical access to the video viewing area is limited to the trained actors, TSA officers, and project staff. Signs are posted around the video collection sites informing airport passengers and personnel that video recording is occurring and instructing persons to walk around the designated areas.

Nonetheless, the primary privacy risk is the unwanted collection and distribution of PII from members of the public who may be near the trained actors as they are filmed. Public passengers and airport personnel may be incidentally captured on video during the data collection process. In this case, no effort will be made to identify the passengers or personnel, or use their information (i.e., behaviors) in this research effort. If a TSA officer engages with an airport passenger during the video data collection process at a collection site while a vignette is occurring, the video data immediately prior to, during, and following the engagement will be deleted.

Video data will be collected from existing CCTV cameras owned and operated by the airport and cameras deployed by S&T. The video data will be viewed by TSA subject matter experts in order to determine whether the behavior indicators exhibited by the trained actors can be observed from the video data. The video data may also be used to test and evaluate algorithms for person and object detection and tracking. The video data may also be used by TSA for training purposes.

In order to perform the data collection, S&T has entered into an agreement with the Rhode Island Airport Commission (RIAC) to collect, store, and transport video data. Data collected by S&T will be stored in a secure DHS facility. The RIAC will retain ownership rights to all video data collected and will ultimately determine with whom any video data collected can

be shared. If DHS determined that there is no longer a need for the collected video data, it will be destroyed.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Air Transportation Security Act of 1974 directed that U.S. airport operators establish security programs that include law enforcement personnel from state, local, and private sources. The law mandated that the Department of Transportation's Federal Aviation Administration (FAA) prescribe regulations that require weapons detecting screening of all passengers and accompanied property.[3] This law established the basis for screening passengers at airports. The 2001 Aviation and Transportation Security Act established the Transportation Security Administration (TSA) and transferred responsibility for passenger screening and aviation security from FAA to TSA.[4] The Homeland Security Act of 2002 established the Department of Homeland Security and transferred the TSA from the Department of Transportation to DHS.[5] The mission of TSA is to protect U.S. transportation systems to ensure freedom of movement for people and commerce. In order to execute this mission, TSA employs a multifaceted approach to passenger and airport security. The Behavior Detection and Analysis (BDA) program is among TSA's many layers of security. Unlike other layers of security, which focus on detection of objects using state-of-the-art technology, behavior detection involves the human factor by considering the possible intent to do harm.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

A SORN is not applicable because no data is being retrieved using a personal identifier. The trained actors have consented to having their activities video recorded and shared with other government agencies and research organizations.[6] The trained actors will not be re-identified via the consent forms the actors signed, or any other sources of data. No attempt will be made to identify the airport passengers captured in the background of the various scenarios.

TSA may retrieve the video data to study how persons react in specific settings. TSA will not re-identify the actors and TSA will not retrieve the information by unique identifier.

---

[3] Air Transportation Security Act (Summary) (Pub. L. No. 93-366).
[4] Aviation and Transportation Security Act (Pub. L. No. 107-71).
[5] Homeland Security Act (Pub. L. No.107-296).
[6] The consent forms and PII collected from the trained actors is covered by DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN (December 9, 2008), 73 FR 74743, *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-09/html/E8-29059.htm.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

S&T, TSA, and the RIAC are developing an information sharing agreement (referred to as a Data Management Plan) that will identify data security and sharing procedures for the collected data. S&T anticipates that the Data Management Plan will be formally signed by all parties (S&T, TSA, RAIC) in June 2015.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. S&T is collecting video data to create training videos for TSA. The trained actors appearing in the videos have signed consent forms allowing their likenesses to be used for training purposes. Training videos are not considered "records," and are not explicitly subject to data retention and deletion requirements.

TSA may use the training videos for years or even decades to demonstrate similarities and differences in behaviors over short and long periods of time.

TSA will delete the training videos in accordance with NARA General Records Schedule 20 which covers the disposition of electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the files or records. These training records will be deleted or destroyed when "the agency [TSA] determines they are no longer longer needed."

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act does not apply to this data collection effort.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The CHI data collection effort will collect digital video recordings (without audio) of volunteer actors (i.e., persons who have provided written consent to appear in the video

recordings)[7] and traveling members of the public at T.F. Green Airport, PVD. Actors will role-play specific behaviors in an airport environment. The roles portrayed by the actors are based on situational scenarios that TSA identifies as potential evidence of high-risk behavior. Non-actors (the public) who are present while a scenario is being recorded may appear in the video data. The video data (depicting facial and body appearance) is the only PII collected. No additional information is being collected at the airport. The video images incidentally collected from traveling members of the public will not be linked to any information that may identify those individuals. The video data may be shared with TSA and other government agencies for training, test, and evaluation purposes. All sharing requests must be approved by the RIAC.

2.2 What are the sources of the information and how is the information collected for the project?

The video data is collected from overhead CCTV and front facing cameras. The video data collection will occur at the T.F. Green Airport, PVD. Within each video sequence, information content will only be further collected from volunteer actors posing as passengers and acting out various scenarios.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

S&T testing will rely on information based on S&T and TSA staff direct observation from video. S&T and TSA staff will observe and document the behaviors exhibited by the volunteer actors. As such, the information can only be inaccurate if the behavior exhibited is labeled incorrectly during post-analysis. In the context of this research effort, the identity of the individuals from whom PII is collected (e.g., facial and body images) is not considered to be relevant for analysis.

To ensure that the data is not manipulated or otherwise altered, the video data will be secured at a DHS facility and physical and computer security will be employed to limit access. If video data is shared outside of DHS, this Privacy Impact Assessment will be updated accordingly. Per agreement with Providence Airport Authority, the data will only be used for two purposes: (1) validate if video can be used for behavior detection and (2) future TSA BDO

[7] Note that S&T has conducted a full PIA on their use of volunteers in testing environments. For more information, please see DHS/S&T/PIA-020 - Research Projects Involving Volunteers (November 23, 2010), *available at* http://www.dhs.gov/privacy-documents-st.

training. Any other usage will require submission of a written request to Providence Airport Authority.

Data tracking and logging procedures will trace actions undertaken by a user of the data. These procedures will be outlined in an information sharing agreement between S&T, TSA, and the RIAC.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that S&T may collect information from members of the public who have not consented to this collection.

Mitigation: With respect to any incidental capture of images of the general traveling public, S&T will post signs in the area where the data collection is being conducted. The sign will state: "This area is under video surveillance and recording" (or similar). To account for individuals that may not use English as a primary language, pictographic signs will also be posted. These steps will sufficiently inform individuals that a data collection is ongoing.

Privacy Risk: There is a risk that incidental data collected from members of the public does not advance the purpose of this program, which is to develop state-of-the art in behavior detection science.

Mitigation: The TSA Behavior Detection and Analysis program is one of several layers of screening used by the TSA to perform risk-based passenger screening and ensure passenger safety. An observability study promotes value to TSA in that a centralized screening location will offer the ability to expand screening capabilities while reducing staffing costs. A reliability study promotes further value in that behavioral indicators that cannot be reliably observed can be eliminated, which will optimize screening decisions. If S&T and TSA determine that incidental data from members of the public does not advance the purpose of the Behavior Detection and Analysis program, they will develop other tests that will minimize collection of incidental data.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The video data is being collected to test, evaluate, and provide auditing capability of the TSA BDA program. The video data enables researchers to conduct statistical evaluations of BDO operations in a live environment. The observability study will be used to inform whether behavioral indicators can be assessed from remote locations (i.e., via video away from the live scene). This information may be used by TSA to improve BDO training and performance. In addition, the data may be used to develop a dataset to test and evaluate the performance of

tracking algorithms for multi-camera person and object detection to determine a person's path or possible associates in an operational environment.

Subject matter experts will review the video and identify various human behaviors as portrayed by the trained actors. Various detection and tracking algorithms will be used to determine the accuracy of these algorithms. Data is not evaluated or analyzed during the video data collection process. Neither Transportation Security Officers nor BDOs will have access to the video data during a live data collection and the data will not be used to inform any operational decisions.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The data collection effort does not use any technology to conduct electronic searching or record retrieval. The data collection will only use cameras to observe a scene, and later be analyzed by subject matter experts (SME).

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, this data collection also involves TSA. S&T and TSA will collaborate to analyze the video to assess the effectiveness of video as tool to observe and identify behavior and to identify future program directions. The goal of this collaboration will seek to determine whether behaviors could be reliably observed from video. For purposes of this project, the collected PII is incidental.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that collected video data as part of this test may be used to make operational determinations about members of the traveling public.

Mitigation: Although the video collection will collect PII in the form of facial and body images, S&T will not link the video data to an individual. S&T will not be able to use the video data to identify individuals in the collection area while a vignette is ongoing. TSA officers on-site will not see the video data and are not able to use the video data to inform operational decisions.

To further mitigate any privacy risks to traveling members of the public, if a TSA officer engages with an airport passenger during the video data collection process at a collection site while a vignette is occurring, the video data immediately prior to, during, and following the engagement will be deleted.

To ensure security of the data, S&T, TSA, and the RIAC have developed an information sharing agreement that identifies how the data will be collected at the airport, transferred to a secure DHS facility for storage, and further secured for further use.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

With respect to any incidental capture of the general public, S&T will post signs in the area where the data collection is being conducted. The sign will state: "This area is under video surveillance" (or similar). To account for individuals that may not use English as a primary language, pictographic signs will also be posted. These steps will sufficiently inform individuals that a data collection is ongoing. Trained actors reviewed and signed an information consent agreement acknowledging they will be captured on video during role-playing scenarios.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

When possible, individuals will be allowed to proceed to an alternative security checkpoint if they do not wish to risk indirect observation during a planned vignette. However, the T.F. Green Airport, PVD presently employs CCTV surveillance cameras for its own security purposes. DHS does not control the airports use of the cameras. Individuals do not have the opportunity to opt out of general CCTV surveillance from the airport.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals who may incidentally appear in the data collection are not aware of the video data collection and not offered an opportunity to opt out.

Mitigation: Members of the public that may be incidentally captured are provided notice of the data collection via signage and offered the opportunity to avoid the collection area while a vignette is active. Signage is provided in English and in pictographic signs. The actors that are role-playing scenarios have signed informed consent forms agreeing to participate in the video data collection. The privacy risks are mitigated by the fact that the data collected is not linked to any personal identifier and the data is only used to evaluate whether behaviors can be reliably observed and as a test-bed for video analytic algorithms. The data will also be protected by computer and physical security measures agreed upon by S&T, TSA, and the RIAC.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The information from this data collection effort will be retained in accordance with NARA General Records Schedule 3.1, Item 11, guidelines. In the event the data is deemed insufficient (e.g., insufficient quality, or of no value) the data will be destroyed.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a heightened risk that the video data could be lost or otherwise compromised due to the indefinite length of retention.

Mitigation: The video data may be used to train TSA Behavioral Detection Officers for years and possibly decades into the future. The trained actors captured in these training videos have consented to their likenesses being used in training videos for an indefinite time. The video images of the trained actors analyzed by S&T will be retained in accordance with GRS 3.1, Item 11. The data will be destroyed if it is no longer needed, deemed antiquated, or insufficient for analysis or technical development. No PII will be linked to the stored videos. The research effort will only be used to study the observability of human behaviors from various camera angles and to test cross-camera detection and tracking algorithms.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The RIAC owns all video data collected from its CCTV infrastructure and any ancillary video data that is collected by S&T or its contractor. This includes video data that is collected on cameras that are not owned by the airport and brought to the data collection by S&T or its contractor.

DHS will not distribute or share the stored video vignettes collected by S&T of the government facility in which it is stored, unless such distribution is explicitly allowed by agreement of the RIAC, TSA, and S&T. Per agreement with Providence Airport Authority, the data will only be used for two purposes: (1) validate if video can be used for behavior detection and (2) future TSA BDO training. Any other usage will require submission of a written request

to Providence Airport Authority. If video data is shared outside of DHS, this Privacy Impact Assessment will be updated.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

A SORN is not applicable to the CHI data collection effort because neither S&T nor TSA retrieves data using a personal identifier. The PII collected from the trained actors and their informed consent to having their activities video recorded is covered by the DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN.[8] Only video data images may be shared with other government agencies and research organizations, consistent with the Data Management Plan stated in Section 1.3. No PII maintained by the DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN may be shared and the video data images will not be re-identified with the trained actor PII on the consent forms.

6.3 Does the project place limitations on re-dissemination?

The owner of the video data is the RIAC. If an external entity is given permission to access the video data, the entity must secure further permission from the RIAC in order to do so, in addition to securing permission from S&T and TSA.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

While this data is not covered by the Privacy Act and therefore does not have a requirement to account for disclosures outside of the Department, S&T, TSA and RIAC have developed an information sharing agreement referred to as a Data Management Plan, which discusses protocols for sharing and record-keeping. If S&T, TSA, and the RIAC agree to share the video data, the sharing is documented with a mutually approved Data Request Form. Any entity receiving permission to possess a copy of the data must adhere to monthly reporting requirements that are stated within the Data Request Form.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data collected for test purposes may be shared with external entities for a purpose inconsistent with the original collection.

Mitigation: S&T, TSA, and the RIAC have developed a Data Management Plan that outlines the security protocols for the collection, transmission, storage, and sharing of the video data. All parties will agree to the Data Management Plan prior to the data collection.

[8] DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN (December 9, 2008), 73 FR 74743, *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-09/html/E8-29059.htm.

It is possible that S&T or TSA may want to use videos outside of the context of the DHS research. If and when such a situation occurs, the potential recipient of the data must obtain the approval of TSA, S&T, and the RIAC for the data it wishes to obtain. As proof that such approval is obtained, a Data Request Form will be required for any data transfer outside of the research enclave. All relevant information and signatures must be present on the form before any data transfer occurs.

Once an access form is completed, the requested data will be assembled into a package in the same manner as the data collected from the collection site. Since it is intended that a labeled Blu-Ray disc will be the primary means of data transfer from the collection site, the intention is a similarly labeled and organized Blu-Ray disc would be used for data export. A record of the transfer will then be entered into the repository database. This record will include the contents of the data package, the time and technician, and details about the recipient of the data.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The video recordings in this data collection are not linked to any identifying data such as a surname, given name, or otherwise legal name, therefore S&T is unable to provide individuals with access to their information.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The primary information content is created from direct observation and will not be altered in any way. Part of test and evaluation activities includes determining the level of inaccurate or erroneous information being generated. Regardless of the level of inaccurate or erroneous information, the data will not be used by S&T for operational decision making purposes.

7.3 How does the project notify individuals about the procedures for correcting their information?

As the video recordings are collected through direct observation and are not linked to an individual, there are no procedures for correcting inaccurate or erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Members of the public whose images are incidentally collecting during this project do have not an opportunity for redress.

Mitigation: TSA and S&T users will not have the means to identify members of the public from the video images. The information is in the form of a video sequence depicting observed actions. The authenticity of the video data is protected by computer and physical security procedures. Any video data of TSOs or BDOs engaging with non-actors will not be part of the dataset.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The video data collection is subject to the completion of a signed information sharing agreement between S&T, TSA, and the RIAC. The information sharing agreement is referred to as the Data Management Agreement. S&T also requires that the data collection receive Institutional Review Board (IRB) approval or exemption prior to the start of data collection. On March 31, 2015, the IRB concluded that the data collection effort does not involve human subject testing and that an IRB review is not necessary because the video data is collected from (1) volunteer actors and (2) the actors are performing scripted scenarios. The S&T Compliance Assurance Program Office (CAPO) accepted this finding on April 2, 2015.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Each operator, maintainer, and CHI team member will be trained on DHS privacy policies. All DHS employees and contractors with access to DHS technologies and equipment are required to complete annual DHS privacy training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to the video data collected by S&T is limited to CHI team members and SMEs. The video data will only be accessible in a limited-access secure facility. CHI team members will create machine user accounts specifically for individuals conducting research. Individual user accounts will limit access and provide a precise log of researcher (user) actions. Copying of video data will not be permitted except as required for research purposes or disaster recovery. If

the video data is shared with other government agencies or research institutions, the RIAC must first approve the sharing and similar access limitations and security controls will be required.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing agreements are reviewed by the program manager, S&T Privacy Officer, and S&T legal counsel before any information sharing actions take place.

Responsible Officials

Dr. Kai-Dee Chu
Program Manager
Department of Homeland Security

Christopher S. Lee
Privacy Officer
Department of Homeland Security
Science & Technology Directorate

Approval Signature

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security