Privacy Impact Assessment Update
for the

Facial Recognition Data Collection Project

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

September 16, 2013

Contact Point
Patricia Wolfhope
Resilient Systems 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

Introduction

The Department of Homeland Security Science and Technology Directorate (DHS S&T) Resilient Systems Division has funded Pacific Northwest National Laboratory (PNNL) to perform a face video data collection at the at the Toyota Center in Kennewick, WA. S&T is conducting this Privacy Impact Assessment (PIA) to address privacy concerns raised by the collection and use of facial recognition data.

Fair Information Practice Principles (FIPPs)

DHS S&T is responsible for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department. The S&T Resilient Systems Division is collecting facial video data to test and evaluate facial recognition software. The actual identities of the volunteer participants will not be disclosed to any federal government agencies, and the goal of the project is to determine the accuracy of facial recognition software.

The research methodology has been approved by an Institutional Review Board (IRB). Volunteer participants sign informed consent agreements that describe the facial video data collection and uses. The PNNL IRB, an independent committee that reviews research in which people participate, has approved this study.

The volunteers are assigned anonymized subject numbers. The actual identities and anonymized subject numbers are not connected. Volunteers' actual identities are not used in the facial recognition testing. Only facial recognition video data collected for this study will be used to test facial recognition software. The facial recognition video data collected for this project will not be combined with any other collections of data. Facial video data and photographs outside of this study will not be included in the testing process. The goal of this project is determining the accuracy of facial recognition software.

Facial recognition video data collection is being conducted at the Toyota Center in Kennewick, Washington, with consent from the Center's management. The Toyota Center has been used since 2008 as a long-term test bed and data collection facility.

Images of members of the public may be incidentally captured if they walk past designated facial recognition video data collection cameras, but these members of the public will not be identified by facial recognition systems. Notices are posted at the venue to inform the public about the testing and facial recognition video data collection. Alternative routes are provided at the venue, allowing the public to avoid the facial video data collection areas.

Reason for the PIA Update

The *Standoff Technology Integration and Demonstration Program (STIDP) PIA Update* published in December 2012 covers the use of the Standoff Detection Test Bed to test and evaluate video cameras. S&T is updating this PIA to address facial video data collection and facial recognition software testing. This PIA update addresses privacy risks associated with facial video data collection and facial recognition software testing, and how DHS S&T mitigates these risks.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of 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.

Each volunteer is assigned a subject number. The subject number is used for volunteer management and match verification purposes only. No other identifying information is collected from volunteers during the video collection or facial recognition tests. Images of passersby not involved with the collection may incidentally be captured during collection activities. If this occurs, researchers will not match the non-volunteer images to a specific subject number.

DHS S&T has also provided notice to individuals that their images will be collected and possibly shared by participating in this project. The notice states:

> "PNNL will be collecting video data during the event and your image will appear on the video. PNNL will obtain photographs of you and you will also be asked to provide at least one personal photograph of yourself in a natural setting from the past several years. Your facial image is the only personal information that is being used in this study. Your actual name will not be linked to the facial images you provide. PNNL will not keep your name or other identifying information in the research files, other than on this consent form ... PNNL will send the video to another government agency only for research purposes. No personal information, such as your name, will be supplied with this video data, nor will you be identified in any way."

Data is being collected at hockey games held at the Toyota Center. The hockey team management is mailing letters to season ticketholders addressing the the facial video data collection. The letter includes a color-coded map of the Toyota Center, highlighting the locations the data collection is occurring, and the "opt out" lanes where no facial recognition video data collection is occurring. Signs will be posted at the venue on the days facial recognition video data collection is occurring. Signs will also point out detours and "opt out" zones where no facial recognition video data collection is occurring.

PNNL is conducting media outreach activities with the local newspaper and television stations. Through interviews and press conferences, PNNL will describe the facial recognition video data collection activities, and the opt out lanes at the venue. PNNL is distributing a press packet that includes a description of the data collection, a list of Frequently Asked Questions and Answers, and points of contact for additional information.

PNNL is also posting the media materials on its web site, allowing the public to read and review the information.

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.

Volunteer participants sign informed consent agreements that describe the data being collected and the intended uses. Non-volunteers who are incidentally captured on video will not be identified in the collection. Signs will be posted at the venue on the days facial recognition video data collection is occurring. Signs will also point out detours and "opt out" zones where no facial recognition video data collection is occurring. No other facial recognition video data will be included in the facial recognition software testing. The goal of this project is validating the accuracy of facial recognition software.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The facial video data collection and facial recognition testing is being conducted under authority established by the Homeland Security Act of 2002, Title III, Section 302(4), directing DHS S&T to conduct "…basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department…". This project is consistent with the Homeland Security Act of 2002, Title III, Section 302(4), and with S&T's mission of providing research, development, testing, and evaluation to support DHS's goals and missions. The facial video data will help DHS test and evaluate facial recognition software. The testing and evaluation will help determine facial recognition software accuracy and the validity of claims made by software vendors. The actual identities of the volunteer participants is not relevant since S&T is only testing the accuracy of the technology.

4. Principle of Data 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).

The facial video data collection is only being used to test facial recognition software. The data will be retained for the duration of the project and destroyed at the end of testing. Some images of volunteers may be published in reports to demonstrate various capabilities. 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 will not be published or used.

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.

DHS S&T will receive the facial recognition video data collected from volunteer participants, along with a list of anonymized subject numbers to test the data for quality control purposes. DHS S&T may share the facial recognition video data collected from volunteer participants and the list of anonymized subject numbers with other federal government agencies to test facial recognition software. The actual identities of the volunteers and other persons in the venue is not relevant, and will not be provided to DHS or any other federal government agencies. Any passersby who are incidentally captured by the video data collection will not be identified.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Facial video data is collected directly from volunteer participants. Volunteers are assigned subject numbers. Testing will determine how well facial recognition software can match volunteers and their subject numbers. The volunteers will not suffer any consequences if the facial recognition software fails to match their facial images to their subject numbers. No other facial recognition video data will be included in the facial recognition software testing. The goal of the project is to determine the accuracy of facial recognition software.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

S&T is further safeguarding PII by implementing proceedures that help mitigate privacy risks associated with facial recognition. The facial video data will be encrypted to prevent unauthorized use. Access to the data is limited to authorized researchers and support staff. All persons authorized to access to the data are required to complete annual privacy and security training that describes how to protect and safeguard data containing personally identifiable information.

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, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All persons with access to the data are required to complete annual privacy and security training that describes how to protect and safeguard data containing personally identifiable information. The program manager will audit the data collection and usage activities to ensure the data is being used as described, and that privacy and security protections are followed.

Conclusion

DHS S&T is responsible for testing and evaluating technologies that have the potential to support the Department's mission. S&T is collecting facial video data from volunteers who have signed informed consent agreements. The facial video data is used only to test facial recognition software. The actual identities of the volunteers and the other persons in the venue is not relevant to this study. The goal of the project is to determine the accuracy of the facial recognition software. Protections have been implemented to protect the privacy of volunteers, as well as members of the public that may be present during the video data collection. The data collection and testing will help DHS determine the current capabilities and limitations of facial recognition software.

Responsible Officials

Patricia Wolfhope
Program Manager
Department of Homeland Security

Approval Signature Page

Original signed copy on file with DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security