Privacy Impact Assessment
for the

Facial Recognition Pilot

DHS/USSS/PIA-024

November 26, 2018

Contact Point
Timothy Scott
Office of Technical Development & Mission Support
U.S. Secret Service
202-942-3117

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202)343-1717

Abstract

U.S. Secret Service (USSS or Secret Service) will operate a Facial Recognition Pilot (FRP) at the White House Complex in order to biometrically confirm the identity of volunteer USSS employees in public spaces around the complex. The FRP will seek to test USSS's ability to verify the identities of a test population of volunteer USSS employees. Ultimately, the goal of the FRP is to identify if facial recognition technologies can be of assistance to the USSS in identifying known subjects of interest prior to initial contact with law enforcement at the White House Complex. The collection of volunteer subject data will assist USSS in testing the ability of facial recognition technology to identify known individuals and to determine if biometric technology can be incorporated into the continuously evolving security plan at the White House Complex.

Introduction

One of the dual responsibilities of the Secret Service, as defined in 18 U.S.C. § 3056, is protection of the President, Vice President, their families, visiting heads of state, and other designated individuals. Currently, the USSS uses Uniformed Division Officers and Special Agents assigned to the White House to identify subjects of interest[1] that may approach the White House Complex. These officers and agents are currently provided with static photos used to identify subjects of interest. The USSS believes that deploying facial recognition technology will allow USSS law enforcement personnel to conduct a facial comparison prior to interaction or engagement.

The FRP will be conducted in two separate areas of the White House Complex, using video streams from selected cameras taken from the existing USSS Crown Closed Circuit Television (CCTV) camera system.[2] The cameras that will be used are located at USSS posts where USSS officers and/or agents are also posted, and the cameras capture video from individuals on the sidewalk and street.

One of the areas selected for the FRP is in an open setting, where individuals are free to approach from any angle, and where environmental factors will vary (e.g., lighting, distance, shadows, physical obstructions). The second area of the White House Complex provides a controlled flow of individuals, which will be in a lighted area and free from other obstructions. For

[1] Subjects of interest may come to Secret Service attention through direct contact, social media posts made in public forums, reports from concerned citizens, other agency reports, or media reporting. Information acquired through those means is evaluated by personnel trained in threat assessment protocols and may include: physical identifiers, criminal history, health history, employment history, military service history, education history, immigration status, and other personal information provided by the subject or others familiar with the subject.

[2] *See* DHS/ALL/PIA-042 Closed Circuit Television, *available at* https://www.dhs.gov/publication/dhs-all-pia-042-cctv-systems-0.

both locations, the technology used in the FRP will have the ability to capture facial images out to approximately 20 yards. Conducting the pilot in this manner will provide more detailed information as to how the USSS should proceed in regards to the use of facial recognition technology in the future.

The Crown CCTV system will provide video streams from the selected cameras to the FRP database for identity matching. The FRP system will analyze the video streams to identify facial images. The identified facial images will be queried using facial recognition algorithms against the gallery of photos of USSS volunteers used in the pilot. This will result in a "no match" or "match" result. USSS will use this data to test the ability of the FRP database to confirm the identity of volunteer USSS employees using facial biometric comparison algorithms.

Only facial image data that is identified as a match will be retained. If the facial image is determined to be a match, then the facial image will be considered a record and retained for research and development of the FRP system until the conclusion of the pilot, at which point it will be deleted. If the facial image is determined not to be a match, then the image will be deemed a non-record and will be deleted immediately and automatically. All facial images will be utilized only for official business and testing related to the pilot and will not be shared. At the conclusion of the pilot, August 30, 2019, all remaining collected facial image data will be deleted from the system. Deletion of facial image data will take place earlier if the evaluation of the data is complete.

Volunteer USSS employees are being used in the FRP to provide adequate test data. During the pilot, USSS is interested in identifying only volunteer employees. Volunteer USSS employee photos will be loaded into the FRP database for comparison matching and retained in the database for the duration of the test to support project analysis and to inform and improve facial comparison capabilities. The volunteer employees will need to physically move through the two areas for the FRP to generate test data. The volunteers participating in the FRP will provide information regarding their visits to either of the two FRP sites. The USSS personnel and contract support staff conducting the pilot will be reviewing the matches generated by the FRP database and comparing them to the volunteer information to measure accuracy of the system.

USSS employees that choose to volunteer will have the ability to withdraw from the pilot at any time. All volunteers will be briefed on the scope of the pilot and advised that their participation is strictly voluntary. No name will be associated with any facial image. Images will be associated only with a unique case number for the volunteer USSS employees.

When a match is received, an alert will be generated in the FRP database. This alert will be accessible only to USSS employees or contract support staff with access to the FRP system. The alerts will not be monitored in real time, but reviewed by the USSS employees and contract staff conducting the pilot to analyze the generated data. All images identified as a match will be

visually confirmed by USSS personnel. Review of the FRP match images is scheduled to take place weekly. During the pilot there will not be personnel actively monitoring the alerts made by the FRP database. The system will not be staffed 24/7 but rather reviewed weekly. This PIA addresses Phase One of the FRP, which is scheduled to begin on November 19, 2018, and will run until August 30, 2019. USSS will update this PIA, as necessary, to address any future field tests as they are developed and deployed.

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.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to 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.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. This PIA examines the privacy impact of the USSS Facial Recognition Pilot and collection of facial images as it relates to the Fair Information Principles.

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.

USSS is providing transparency to the public through the publication of this FIPPs-based PIA to provide public notice of the deployment of this new technology. USSS employees who volunteer to participate in the pilot will be provided written notice via email. The USSS employee will be advised that there is no penalty if he or she chooses not to participate in the pilot, and will need to provide written consent to USSS personnel operating the pilot if he or she chooses to

participate. If at any time during the pilot the employee wishes to no longer participate, the employee can notify the USSS employees who are conducting the pilot and request removal. Once the FRP is complete, the USSS may determine that the technology will be used at other locations at the White House Complex. Secret Service will issue a new or updated PIA if USSS decides to move forward with the use of the technology beyond the pilot.

Privacy Risk: Individual members of the public may be unaware that their facial images are being captured and used by a facial recognition technology.

Mitigation: This risk is partially mitigated. General notice is provided to the public by this PIA. The USSS volunteer employees participating in the pilot are provided individual notice and have consented to their participation. Facial images determined not to be a match to images in the USSS gallery will be immediately deleted from the FRP system.

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.

The FRP will receive video streams from the existing Crown CCTV system. The cameras used for the Crown CCTV system can be seen mounted on pole structures. These streams will be from two separate locations on the White House Complex, and will include images of individuals passing by on public streets and parks adjacent to the White House Complex. The FRP system will then analyze the video streams to identify facial images. The identified facial images will be queried against the gallery of photos used in the pilot. This will result in a "no match" or "match" result. Images that generate a "no match" will not be retained for any length of time.

Privacy Risk: There is a risk to individual participation because members of the public cannot opt-out of the FRP testing.

Mitigation: This risk is not mitigated. The White House Complex is a highly monitored area with existing CCTV capabilities. Individuals passing the cameras involved in the pilot will not be able to opt out of having their faces run against the facial recognition algorithm. However, individuals who do not wish to be captured by White House Complex CCTV and cameras involved in this pilot may choose to avoid the area.

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 data collected during the FRP will be used by USSS to assess facial comparison capabilities. During the FRP, USSS will be looking to identify only USSS volunteers, but the data generated will assist the USSS in making the determination to move forward with use of the facial recognition technology. The pilot will look to identify if the use of facial recognition technologies will improve the ability of the USSS to verify subjects of interest prior to direct engagement with law enforcement at the White House Complex.

Privacy Risk: Facial images collected by the test could be used for purposes other than those specified above.

Mitigation: The data collected will be stored in a stand-alone FRP database dedicated to this pilot testing and not made available for routine use in supporting USSS operations. Upon completion of the FRP all remaining collected facial images will be deleted. Images collected by the pilot that become part of a case file for a law enforcement investigation or encounter are governed by the DHS/USSS-001 Criminal Investigation Information System SORN[3] and DHS/USSS-004 Protection Information System SORN.[4] Individuals who believe their images may have been used in a law enforcement investigation or encounter must follow the procedures outlined in the corresponding privacy documents for DHS/USSS-001 and DHS/USSS-004 SORN.

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 images of volunteer USSS employees, used as a baseline for comparison, will be associated with a sample case number for the volunteer USSS employees. The facial images will be kept in a secure, on-site location, and cannot be accessed outside of the White House Complex.

The FRP will obtain facial images that will be compared against the baseline images from individuals passing in proximity to two separate areas at the White House Complex. The NARA-

[3] *See* DHS/USSS-001 Criminal Investigation Information SORN, 76 FR 49497 (August 10, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.
[4] *See* DHS/USSS-004 Protection Information Systems SORN, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

approved schedule DAA-0087-2014-0001, Security Camera Recordings and Associated Data, requires that the corresponding video streams be destroyed after 30 days unless related to an unusual incident or open law enforcement matter.

Non-matching images will be deemed non-records and will be immediately destroyed. Facial images that generate a match in the FRP database will be retained on the server until the completion of the pilot.

Facial images collected by the FRP will only be matched against the images of USSS volunteers, and will not be used for any additional enforcement checks. The FRP will not collect any additional information on individuals. The FRP database will not include the names or any other form of PII on the volunteer USSS employees.

The collection of data will assist the Secret Service in testing the ability to identify individuals with facial images and to determine if biometric technology can be incorporated into the continuously evolving security plan at the White House Complex. At the conclusion of the pilot, August 30, 2019, all remaining collected facial image data will be deleted from the system (deletion of facial image data will take place earlier if the evaluation of the data is complete), consistent with General Records Schedule 3.2 item 010, which permits test files and data to be deleted when no longer needed for agency/IT administrative purposes. Based on the results of the pilot, the USSS will coordinate with DHS any appropriate amendments to existing records retention schedules.

Privacy Risk: There is a risk that test data might be stored longer than is necessary.

Mitigation: The Secret Service will use the data from the FRP only for the evaluation, unless the data is associated with an open law enforcement matter. Facial images captured during the pilot will be deleted by August 30, 2019. The FRP will be continually evaluated during the operational pilot and will delete the data earlier when it is determined that the data is no longer needed.

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.

This pilot will be used to determine the viability of facial comparison technology and data system processing in the area around the White House Complex. Facial images extracted by the FRP will assist the Secret Service in testing the ability to accurately identify individuals using facial images and to determine if biometric technology can be incorporated into security measures at the White House Complex and potentially additional protected sites in the future. The USSS

will not share any of the facial image data it collects with any party outside of DHS, unless there is a legal obligation to do so.

Privacy Risk: There is a risk that data may be inappropriately accessed.

Mitigation: The FRP database will reside on the White House Complex, and will not be able to be accessed remotely, even by USSS personnel. DHS elements outside of USSS cannot access test data. All data collected by the FRP will be deleted no later than August, 30, 2019, unless it is associated with an open law enforcement matter. The USSS takes precautions to prevent the alteration or deletion of the facial image data to ensure that all information is accurately captured and retained. The data will be stored on a USSS-approved server, which will only be accessible by authorized USSS users. The data is for official use only and is prohibited from being downloaded, manipulated, or otherwise used for personal use.

Privacy Risk: There is a risk that the data will be used outside of the USSS.

Mitigation: The FRP data is retained on a stand-alone server that will support only this pilot. Only a limited number of USSS employees and cleared contract support staff will have access to the data. At the conclusion of the pilot, all facial image data will be deleted, unless it is associated with an open law enforcement matter.

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 image data is captured in real time from the CCTV cameras to obtain an accurate image of the individual. For both locations on the White House Complex the FRP database will have the ability to capture facial images up to approximately 20 yards, based on the focal point of the static camera. All cameras used for the pilot will be static, without any zoom or pan capability. USSS personnel are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data during the test. Safeguards are built into the database to prevent unauthorized individuals from altering or deleting facial image data, and to ensure that all information is accurately captured and retained.

Privacy Risk: A facial image received from the video stream may incorrectly show as a match to test data, resulting in member of the public facial images being retained.

Mitigation: This risk is not fully mitigated, as there is always a risk of false positive matches. However, this pilot will look to identify ways to mitigate false positive alerts. As there is a limited gallery of individuals against whom to match, the false positive rate may be limited as well. During the pilot, each image identified as a match will be confirmed by USSS personnel operating the pilot. All FRP images identified as a match will be visually confirmed by trained

USSS personnel on a weekly basis. Additionally, any images that are a match will only be retained until the conclusion of the pilot and no operational use will be made of any matches.

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.

Facial images that generate a match in the FRP database will be retained on the server until the completion of the pilot. At the completion of the pilot the facial images will be deleted, unless they are associated with an open law enforcement matter. Facial images that do not generate a match will not be retained for any length of time.

The facial image data is only stored on a USSS-approved server which is only accessible by USSS personnel and supporting contract support staff. All personnel who have access to the facial image data have had background investigations completed. The facial image data is for official use only and is prohibited from being downloaded, manipulated, or otherwise used for personal use. The FRP server is not accessible remotely, and will physically be housed on the White House Complex. All personnel having access to the server will have individual log-in and passwords associated with each account, and the appropriate logs will be maintained within the system. The USSS is responsible for the FRP data security and protection.

Privacy Risk: There is a risk that unauthorized individuals may see the test data.

Mitigation: All data collected is only viewable in a secure location on the White House Complex. Only the USSS personnel and supporting cleared contract personnel responsible for evaluating the test will see the data. The data will be stored on a standalone server that cannot be accessed remotely.

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 personnel with access to the facial image data are required to complete annual privacy awareness training. USSS employees and contractors must pass a full background investigation and must also be trained regarding the access, use, maintenance, and dissemination of PII before given access to the system containing facial image data. The facial image data will not be accessed

or released for any unauthorized use. USSS will document the deletion of the test data at the conclusion of the pilot.

Privacy Risk: There is a risk that USSS personnel might handle the data in an inappropriate manner.

Mitigation: Only individuals cleared by USSS will have access to the collection database. All USSS personnel and supporting contractors with access to the data undergo annual privacy awareness and document security training. Additionally, only a limited number of personnel will have access to this data, and the USSS will strictly monitor that access is given only to individuals assisting with the evaluation of the pilot.

Conclusion

USSS will conduct regular self-assessments to verify compliance with its responsibilities and the privacy risk mitigations discussed in this PIA. This PIA will be updated as USSS' methods and policies for the use of facial recognition technology evolve.

Responsible Officials

Timothy Scott
Office of Technical Development & Mission Support
U.S. Secret Service

Approval Signature

[Signed copy complete and on file with the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security