Joseph Di Pietro

Chief Technology Officer
Office of Technical Development and Mission Support
United States Secret Service

Written Testimony

Before the
United States House of Representatives
Committee on Homeland Security

July 10, 2019

Good morning Chairman Thompson, Ranking Member Rogers, and distinguished Members of the Committee. I am Joseph Di Pietro, Chief Technology Officer of the United States Secret Service (Secret Service). I want to thank you for the opportunity to appear before you today to discuss the Secret Service's use of biometrics in performance of our integrated mission.

As previously conveyed to your Committee staff, we have serious concerns about testifying in an open hearing on how we use facial recognition technology to enhance our protective mission. Therefore, my testimony today on that issue will focus solely on the current pilot program we have in place at the White House Complex, as outlined in the Department of Homeland Security (DHS) Privacy Impact Assessment (PIA) dated November 26, 2018.

Pursuant to Title 18 U.S.C. § 3056, the Secret Service is authorized to protect the President, the Vice-President, their immediate families, and other individuals enumerated in the statute. It is our responsibility to constantly research and evaluate the benefits and risks of applying available, new and emerging technologies to keep our protectees safe and to enhance the capabilities of our front line Uniformed Division Officers, special agents, and mission support employees.

The Secret Service closely guards our "means and methods" as to how we execute our protective mission. It would not be wise or prudent to discuss in a public setting certain assets, capabilities, and protocols used to carry out our protective mission. We are aware that our adversaries are constantly probing us and could potentially exploit information discussed in this open environment to attack us.

The Secret Service uses biometric tools such as fingerprint analysis and DNA collection on a regular basis, in accordance with standards and policies, in order to investigate, locate, and sometimes arrest individuals who have committed crimes, to include offenses related to threats against Secret Service protectees.

Facial recognition technology is an effective tool that has the potential to act as a force multiplier. Accordingly, the Secret Service seeks to utilize and harness these important advances to enhance our effectiveness while upholding rights guaranteed by our Constitution.

Fingerprint/Palm Prints

The Secret Service has a longstanding fingerprint and palm print program that plays an integral part in our investigative and personnel security processes. The Secret Service's ability to process, store, search, and retrieve fingerprint and palm print images is an operational necessity.

The Secret Service Live-Scan Program (SSLSP) is an enterprise-wide initiative deploying Live-Scan Booking Stations to Secret Service offices agency wide. Live-Scan Booking Stations electronically capture, digitize, and transmit descriptive information, fingerprints, palm prints, signatures, and photos of both applicants and investigative subjects who are processed through these stations. The records are transmitted to the Federal Bureau of Investigation's (FBI) Next Generation Identification System (NGI) database for an automated search against over 76 million criminal fingerprint records. Simultaneously, these records are submitted to the Secret Service's own database for searching and archiving. The conduit used to forward the information to the FBI is the U.S. Department of Justice's Joint Automated Booking System (JABS).

During the course of investigations involving fingerprint and palm print evidence, forensic examiners at the Secret Service utilize a variety of regional and national databases to search latent prints for matches to known subjects. For example, the Secret Service coordinates directly with the FBI and the DHS via their databases, to include the DHS Office of Biometric Identity Management's Automated Biometric Identification System (IDENT).

DNA

DNA evidence is one of the most effective identification tools available to law enforcement today. Advances related to DNA technology have been rapid, and the Secret Service remains dedicated to utilizing new applications to enhance our integrated mission. DNA technology can provide accurate identification, improve prosecution rates, and act as a deterrent against future criminal acts.

The Secret Service collects DNA samples along with a subject's fingerprints as part of the identification and arrest process. Buccal collection kits from the FBI are used during the booking process and are then returned to the FBI for DNA testing, search, and storage in the national DNA database.

Facial Recognition Technology

In 2014 former Secretary of Homeland Security Johnson established an independent Protective Mission Panel (PMP) to conduct an assessment of the security at the White House complex. Among other important recommendations, the PMP stated that, "[t]echnology systems used on the complex must always remain on the cutting-edge, and the Secret Service must invest in technology, including becoming a driver of research and development that may assist in its mission."[1]

Facial recognition technology is a significant tool currently being used with great effectiveness in both the private and government sectors. Accordingly, the Secret Service is evaluating the potential benefits of this technology to this agency's protective mission. Applied correctly and with appropriate controls, this technology could potentially be used by the Secret Service to enhance our security posture at critical protective venues.

Specifically, this technology may have the potential to provide an early notification to Secret Service personnel of individuals who are of record with the agency when they approach a protective site. These individuals would have already made a threat against one of our protectees or been shown to have expressed an "unusual interest" towards one of our protectees and, therefore, pose a serious threat to protected persons, venues, or the general public in close proximity to one of our protected sites.

While the benefits of technology associated with facial recognition may provide greater capabilities than the observations of law enforcement personnel, the Secret Service is well aware that there must be an appropriate balance between security and any potential privacy or other constitutional concerns. Further, it is noted that the Secret Service expects to come in contact with thousands of the general public around the White House every day and that the men and women of the agency strive to ensure a secure environment while respecting all individual's constitutional rights.

---

[1] See *Executive Summary to Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security*, 2014, p. 7.

Facial Recognition Pilot (FRP)

In furtherance of the 2014 PMP report recommendations, the Secret Service Office of Technical Development and Mission Support is currently working on a Facial Recognition Pilot (FRP). The goal of the FRP is to determine whether facial recognition technology could be effectively deployed to enhance the Secret Service's protective mission. In addition, the Service will determine whether this technology would be a fiscally responsible investment that would assist in identifying subjects of interest to the Secret Service as they approach a protected site.

While the FRP started in December 2018 and is scheduled to be completed by the end of August 2019, the Secret Service began contemplating this pilot in August 2014. Prior to the initiation of the program, DHS approved and published a Privacy Impact Assessment, evaluating the privacy risks and associated mitigation strategies.[2]

The participants in the FRP are Secret Service employees who volunteered to take part. These individuals had their images loaded into the FRP server. Video streams capture the volunteers as they move through various locations around the White House Complex, and images of the volunteers are matched to the video streams. Subsequently, volunteers provide notification of their movements in and around the Complex for comparison with the generated matches in the system.

The video streams feed into both the White House CCTV system and into the FRP server. The FRP server is operated on a closed network and is *not* capable of remote connections. The data collected is stored in a stand-alone database dedicated only to the pilot testing. Only individuals cleared by the Secret Service have access to the collection database, and they are accompanied by agency personnel while accessing the FRP server. All Secret Service personnel and supporting contractors with access to the data undergo annual privacy awareness and document security training. Facial images are stored when associated with a match to one of the volunteers, and, at the conclusion of the FRP, all images will be purged.

The data collected throughout the FRP will be evaluated for its effectiveness and accuracy.

Office of Biometric Identity Management (OBIM)

The Secret Service recognizes the value offered by OBIM and its biometric data storing, matching, and sharing capabilities to assist with both our protective and investigative functions. Developing a partnership with OBIM will provide a valuable means to search, match, and store our biometric data across DHS components as well as with external agencies. The Secret Service maintains coordination with OBIM liaisons and continues to develop capabilities and policies regarding the use, storage, and dissemination of biometric information.

Conclusion

[2] DHS/USSS/PIA-024 Facial Recognition Pilot (Nov. 26, 2018).

The protection of our nation's leaders is paramount to this agency and to the nation. The partnerships represented here today, both in Congress and among those of us within DHS, are critical to the success of Secret Service operations. I thank you for the opportunity to testify concerning the agency's use of these evolving technologies, and I look forward to working with you as we move forward.

Chairman Thompson, Ranking Member Rogers, and distinguished Members of the Committee, this concludes my testimony. I welcome any questions you have at this time.