Privacy Impact Assessment

for the

USSS Use of Facial Recognition Technology

DHS Reference No. DHS/USSS/PIA-033

September 12, 2024

Homeland Security

Abstract

The United States Secret Service (USSS or Secret Service) is conducting this Privacy Impact Assessment (PIA) because Secret Service personnel may use facial recognition technology (FRT) during law enforcement activities that fall within Secret Service's jurisdiction. Use of facial recognition technology requires the collection and maintenance of personally identifiable information (PII): facial images. Use of facial recognition technology assists Secret Service law enforcement personnel with developing investigative leads involving suspected criminals engaged in counterfeiting, financial crimes, and cyber-enabled crimes. Pursuant to an authorized criminal investigation, Secret Service personnel assigned to a case may utilize the DHS Office of Biometric Identity Management's Automated Biometric Identification System (IDENT),[1] and other government agency facial recognition technology, through which photographs and/or still video images are used for database searches or one-to-one comparisons to potentially generate investigative leads. The Secret Service does not use commercially provided facial recognition services. This Privacy Impact Assessment will discuss the potential privacy risks of using facial recognition technology for criminal investigative purposes.

Introduction

The investigative mission of the Secret Service is to detect and arrest individuals who are suspected of engaging in crimes that undermine the integrity of U.S. financial and payment systems. During criminal investigations, Secret Service Office of Investigations (INV) personnel may require the identification of potential victims of crimes (e.g., identity theft) or of individuals suspected of crimes. Pursuant to an authorized Secret Service investigation, Secret Service Office of Investigations personnel may submit available photographs or video stills of unknown persons relevant to an investigation as probe images (i.e., facial images or templates) to search against other images or templates using OBIM's or other government agencies' facial recognition technology.

OBIM, or the other agencies, will query their image galleries and may provide lists of images of potential matches to Secret Service Office of Investigations. Secret Service Office of

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available* at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim. DHS is in the process of replacing the Automated Biometric Identification System with the Homeland Advanced Recognition Technology System (HART) as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about the Homeland Advanced Recognition Technology System, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1 AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Investigations personnel may use the potential matches in conjunction with other information relevant to the investigation to produce investigative leads that may assist in the identification of potential victims or suspects. Secret Service Office of Investigations personnel also may request another government agency to conduct a one-to-one comparison of two photographs or video stills pursuant to an authorized Secret Service investigation. Any coordination between Secret Service and other government agencies for use of facial recognition technology will be conducted pursuant to an underlying agreement, including appropriate privacy safeguards.

Facial Recognition Technology

Facial recognition technology uses specialized algorithms to analyze human faces captured in photographs or video footage and compare them to other facial images. Specifically, facial recognition is the automated comparison of facial images based on system-evaluated similarity.[2] Facial recognition technology can be used to identify a potential match to an unknown individual by querying an entire image gallery to find images similar to a submitted image (one-to-many match or candidate list) or to assess similarities between known images of the same person (one-to-one match). An image gallery is a facial recognition system database, which typically contains templates developed from images of known (and possibly unknown) individuals.

Facial recognition technology operates with greater accuracy when there are fewer variables between images. This often requires, for example, ensuring that lighting conditions in the submitted image are like those in which the compared images were taken. Controlled (or constrained) images also reduce variables because they are captured in accordance with facial identification or facial recognition standards or guidelines. Common examples of controlled (or constrained) images are mugshots and visa photographs. Uncontrolled images are not intentionally captured in accordance with facial identification or facial recognition standards or guidelines and are at a greater risk for inaccurate matches.[3] With respect to the Secret Service, uncontrolled (or unconstrained) images are typically photographs or video stills collected through investigative processes and activities.

Prior to using any facial recognition technology, Secret Service personnel must first make reasonable efforts to identify the individual through other existing means and methods, such as government database queries, open-source research, and other routine investigative techniques based on biographical and other non-biometric information. Secret Service personnel may use

[2] *See* ORGANIZATION OF SCIENTIFIC AREA COMMITTEES FOR FORENSIC SCIENCE, STANDARD TERMINOLOGY FOR DIGITAL AND MULTIMEDIA EVIDENCE EXAMINATION (2022), *available at* https://compass.astm.org/document/?contentCode=ASTM%7CE2916-19E01%7Cen-US&page=1.

[3] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, ONGOING FACE RECOGNITION VENDOR TEST (FRTV) PART 2: IDENTIFICATION (2018), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

facial recognition technology to generate candidate lists as investigative leads which require corroboration and may not be used solely as the basis of enforcement action by Secret Service.

All facial recognition technology queries and probe images will be documented and stored in incident-based reporting (e.g., Field Investigative Reporting System (FIRS)[4]). Candidate lists resulting from facial recognition technology queries will also be retained therein.

Accuracy Rates

Facial recognition technology accuracy is measured in terms of two interrelated error rates: the determination that images of two different individuals are images of the same person (false positive or false match) or the determination that two images of the same person are different (false negative or false non-match). The match/no match determinations are based on thresholds that are established by the algorithm's user. Error rates are influenced by the data used and the algorithm. Further, error rates in operation can differ from error rates produced in laboratory testing using curated databases. Standards exist for both laboratory testing (ISO/IEC 19795-1:2021) and operational testing (ISO/IEC 19795-6:2012).

Similarity Scores

Facial recognition technology compares templates of facial images to determine their similarity, which the technology represents using a similarity score. Similarity scores are specific to the algorithm and operational implementation of the facial recognition technology. The technology often performs one of two types of comparisons. The first comparison is known as a one-to-many or identification search, in which the technology uses a probe image to search an image gallery to find potential matches. A probe image is the facial image or template used to search against the image gallery in a facial recognition system. In many cases, the system returns candidates that meet or exceed a certain threshold that are then reviewed by human Facial Examiners. Candidate lists must be reviewed by a trained examiner and compared against corroborating information before any action may be taken against a person.

The second type of comparison is known as one-to-one or verification, a search in which the technology compares a single image to an image or multiple images of a single individual. The face images are considered a match if their similarity score meets or exceeds a certain threshold. The matching will be followed by an evaluation by a trained human examiner if the match is to be used for a Secret Service investigative purpose or enforcement action. One-to-one searches are often used as verification searches for access control situations, for example.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. SECRET SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE FIELD INVESTIGATIVE REPORTING SYSTEM (FIRS), DHS/USSS/PIA-009, *available at* https://www.dhs.gov/privacy-documents-us-secret-service.

Secret Service Use of Facial Recognition Technology

Secret Service Office of Investigations personnel may only use approved facial recognition technologies in a manner consistent with DHS and Secret Service policies. The Secret Service Office of Investigations Criminal Investigative Division (CID), in consultation with the Secret Service Office of the Chief Counsel and Secret Service Privacy Office, is responsible for the facial recognition technology approval process, to include compliance with DHS directives and any additional approval required by DHS. The Secret Service Office of Investigations minimizes the privacy impacts of using facial recognition technology through safeguards similar to those used for use of other personally identifiable information, sensitive personally identifiable information, and law enforcement sensitive (LES) information collected and maintained pursuant to an authorized Secret Service criminal investigation.

Secret Service may only use facial recognition technology pursuant to an authorized ongoing Secret Service investigation, or in support of another agency to support an investigation with a nexus to the Secret Service mission. The process of using facial recognition technology includes an initial selection of probe images by the Secret Service Office of Investigations personnel, the submission of the probe images by Secret Service Office of Investigations personnel to an approved government agency facial recognition technology, the receipt of candidate images resulting from the facial recognition comparison, human review of the purported matches, and further investigation to identify individuals before any action may be taken. This process will be documented in the respective case file.

State, Local, Tribal, and Territorial Facial Recognition Technology

It is customary for law enforcement agencies to share information or allow other law enforcement agencies to submit biographic, descriptive, or other information to query their databases, to include image galleries. Many law enforcement agencies have developed a service allowing external law enforcement agencies to submit probe images to generate candidate lists from their image galleries, including the Secret Service in support of an open and authorized Secret Service investigation.

The Secret Service Office of Investigations frequently works in partnership with state, local, tribal, and territorial law enforcement agencies, both in the form of joint investigations and in a supporting capacity. USSS only provides facial recognition technology support to these agencies in investigations with a nexus to the Secret Service's mission. Many state, local, tribal, and territorial law enforcement agencies throughout the United States maintain large galleries of images collected during law enforcement actions (i.e., mugshots). If permitted by law, some of the agencies also connect directly to their associated Department of Motor Vehicles (DMV) databases to allow for biometric querying of Department of Motor Vehicle information.

Regional and Subject Matter-Specific Intelligence Fusion Centers

Transnational crime and criminal organizations expand beyond local or state jurisdictions. Therefore, many law enforcement agencies have partnered to create fusion centers to collaborate and deconflict law enforcement activities regarding specific crimes.[5] Fusion centers typically receive, gather, analyze, and share threat-related information among state, local, tribal, territorial, federal, and private sector partners.

Certain fusion centers also have data analytic capabilities that aid investigators in processing and visualizing evidence, to include photographs collected during law enforcement activities. The fusion centers may submit probe images to the Secret Service in support of an open and authorized Secret Service investigation. In addition, fusion centers may make available their facial recognition technology to assist Secret Service law enforcement personnel with developing investigative leads involving suspected criminals engaged in counterfeit/financial crimes and cyber-enabled crimes.[6]

Federal Agency Facial Recognition Technology

Office of Biometric Identity Management (OBIM) Facial Recognition Technology

The Automated Biometric Identification System (IDENT), to be replaced by the Homeland Advanced Recognition Technology System (HART), is the designated DHS system for the storage and processing of biometric data. IDENT/HART stores and processes biometric data, fingerprints, facial images (photographs), and iris scans, with associated biographic information to establish and verify identities. OBIM has established interoperability with the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) System[7] and the Department of Defense's (DoD) Automated Biometric Identification System (ABIS)[8,9] to enable data sharing across the biometric enterprise consistent with information sharing agreements and applicable privacy safeguards. OBIM identifies each collection by data provider and for which purposes the information may be used, for how long it may be retained, and with whom it may be shared data.

---

[5] *See* https://www.dhs.gov/fusion-centers.

[6] While the USSS does not have investigative jurisdiction for crimes against children, it is authorized to provide forensic and investigative assistance to the National Center for Missing & Exploited Children and state and local law enforcement.

[7] *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION INDENTIFICATION-INTERSTATE PHOTO SYSTEM, *available at* https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

[8] *See* A0025-2 PMG (DFBA) DoD - Defense Biometric Identification Records System, 80 Fed. Reg. 8292 (Feb. 17, 2015), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/581425/a0025-2-pmg-dfba-DoD/. See A0025-2 SAIS DoD - Defense Biometric Services, 74 Fed. Reg. 48237 (Sept. 22, 2009), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569938/a0025-2-sais-DoD/.

[9] At this time, DHS cannot search ABIS via IDENT. DoD can search IDENT and match responses are provided back to ABIS. The functionality for DHS to search ABIS is expected to be available in HART.

IDENT/HART can restrict queries of its database on request of the data provider and only enables sharing with authorized users after the data provider has approved the sharing on either a one-time or recurrent basis. The Secret Service Office of Investigations submits probe images to IDENT/HART manually through OBIM's Biometric Support Center (BSC) consistent with DHS and Secret Service policies and procedures.

Department of State (DoS) Consolidated Consular Database (CCD)

The Consolidated Consular Database is the Department of State repository for visa and passport records.[10] The Consolidated Consular Database stores information about U.S. citizens and Lawful Permanent Residents (LPR) who have filed passport applications. It also contains information on foreign nationals who have filed immigrant and non-immigrant visa applications. The Consolidated Consular Database may also contain additional information submitted by federal agencies responsive to background checks on an individual. The Consolidated Consular Database provides a facial recognition technology comparison against its database of visa records. It may not retain USSS probe images.

FBI Next Generation Identification (NGI) Interstate Photo System

The Next Generation Identification Interstate Photo System is the FBI's primary identity management system. It contains biometric (i.e., photographs and ten-print fingerprints) and criminal history records of individuals arrested by law enforcement agencies, and submitted to the FBI for criminal justice, national security, and civil purposes. The system has over 38 million photos that are each associated with a 10-print fingerprint scan. The Next Generation Identification Interstate Photo System provides a facial recognition query capability to domestic law enforcement agencies to compare probe images against its image gallery. The FBI may not maintain Secret Service probe images within the Next Generation Identification Interstate Photo System.

Department of Defense (DoD) Automated Biometric Identity System (ABIS)

The Automated Biometric Identity System is the DoD's authoritative biometric system for matching, storing, and sharing biometrics in support of military operations, and has the functionality to conduct facial recognition queries. The Automated Biometric Identity System contains biographic, biometric, and encounter information on known or suspected terrorists, individuals deemed national security threats, current and former DoD detainees, as well as foreign nationals who were screened for security purposes to work on a U.S. military base/facility overseas. The Automated Biometric Identity System shares information with other federal agencies, including the Secret Service, and the DoD's foreign partners. The Automated Biometric Identity System encounter information may contain data elements such as: the Automated

[10] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (CCD), *available at* https://www.state.gov/privacy-impact-assessments-privacy-office/consular-consolidated-database-ccd-pia/.

Biometric Identity System encounter specific identifier, reason fingerprinted, date fingerprinted, associated derogatory information, the fingerprinting agency, associated biometrics (e.g., fingerprints, photos), name, aliases, date of birth, place of birth, country of citizenship, and gender.

Probe Photos

The Secret Service Office of Investigations may use available photographs or video stills collected during and directly relevant to an authorized investigation as probe images for submission to a facial recognition technology. Probe images must be directly relevant to an active investigation for crimes that the Secret Service Office of Investigations has statutory authority to enforce. The Secret Service Office of Investigations may collect a range of photographs during an investigation, such as mugshots, surveillance photos, social media posts, and images seized from electronic devices or obtained from service providers using legal processes. The Secret Service Office of Investigations may also isolate still frames from videos or streaming media to create a probe image.

Most images collected by the Secret Service Office of Investigations will be uncontrolled (or unconstrained) images, often derived from investigative processes and activities. Some variations within uncontrolled images can be reduced, for example, by isolating the facial image from the overall photo. The Secret Service Office of Investigations will select isolated images that are best suited to be probe images for the facial recognition processes. Personnel will make the best attempt to ensure the facial image is isolated with the highest image quality possible, containing the fewest obstructions to the subject's face, and most like a controlled image considering variables such as angle, lighting, distance, and the subject's expression.

In limited circumstances, the Secret Service Office of Investigations may collect controlled images and use a facial recognition technology to verify the asserted identity of an individual, such as in suspected identity theft cases. For example, personnel may submit a passport photo to another government agency for facial recognition purposes to determine if that individual is a possible match to other images and biographic information held by that government agency.

Submission of Probe Images

Probe images will only be used in furtherance of an active, authorized Secret Service investigation. Prior to using facial recognition technology, the Secret Service Office of Investigations will first make reasonable efforts to identify the individual through other investigative processes and activities.

As noted, the Secret Service Office of Investigations may use other government agency facial recognition technology and their corresponding image galleries. Each agency oversees and operates the technology and maintains its image galleries. The Secret Service Office of Investigations personnel will either submit the probe image manually (e.g., via encrypted email) and a representative of the recipient agency will then input the image into their image gallery to

use the facial recognition technology, or will upload the image directly to the facial recognition technology via a web interface. The Secret Service probe image may not be retained by the other agency or by IDENT/HART. The Secret Service Office of Investigations personnel may only supply the minimum information required by the facial recognition technology to run the query, such as a case number.

Receipt and Vetting of Candidate Images

The Secret Service Office of Investigations may not take enforcement action against individuals based solely on facial recognition technology-generated candidate lists. The Secret Service Office of Investigations primarily uses one-to-many query functionalities to generate candidate lists to assist with identifying an unknown person or to locate a person who may have multiple names or identities.

Candidate lists will be used only to develop potential investigative leads. Investigative leads developed from candidate lists are information with varying levels of credibility and may never be used as the sole basis to establish probable cause or determine wrongdoing. In addition, candidate lists are generally accompanied by a disclaimer reminding the recipient that use of facial recognition technology is for lead generation purposes only and outputs are not to be considered as positive identification and are not to be used as the sole basis for any law enforcement action For example, OBIM's IDENT/HART disclaimer is as follows: "The images and information contained in this candidate list are for investigative lead purposes only, are not to be considered as positive identification, and are not to be used as the sole basis for any law enforcement action. Other information must be examined and considered prior to making a determination regarding the true identity of the individual in the submitted probe photo."

Upon receipt of candidate lists, Secret Service Office of Investigations personnel will compare them to other information derived throughout the investigation to determine if any of the candidates can be corroborated by other evidence. This process is known as vetting. The facial recognition similarity scores, if provided, may only be used as a reference for the vetting process by Secret Service Office of Investigations personnel, not as confirmation of an identification. Secret Service Office of Investigations personnel will evaluate candidate returns through non-biometric investigative processes (i.e., human review and corroboration).

If a lead is created because of a vetted match and is then combined with other evidence to establish probable cause in an investigation, personnel may be required to testify to their use of facial recognition technology in a court proceeding. Secret Service Office of Investigations personnel may also use vetted facial recognition matches to establish probable cause in affidavits for warrants to explain how Secret Service initially identified a subject. Information related to Secret Service Office of Investigation's use of the facial recognition technology would also be subject to criminal discovery rules.

Retention and Disposition

Information generated by facial recognition technology and the corresponding vetting and investigation process will be documented in an investigative case file in the Secret Service Field Investigative Reporting System, consistent with Secret Service Office of Investigations policy and federal law. Information that becomes part of an investigative case file will be retained for a period that corresponds with the DHS Records Control Schedule DAA-0087-2021-0001, pending approval by the National Archives and Records Administration (NARA).

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 [11] 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.[12]

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.[13] The Fair Information Practice Principles 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[14] and the Homeland Security Act of 2002, Section 222.[15] Secret Service Office of Investigations utilizes facial recognition technology as a mechanism to develop subject leads related to Secret Service criminal investigations. This Privacy Impact Assessment examines the privacy impact of Secret Service use of facial recognition technology as it relates to the Fair Information Practice Principles.

[11] 5 U.S.C. § 552a.
[12] 6 U.S.C. § 142(a)(2).
[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[14] 44 U.S.C. § 3501 note.
[15] 6 U.S.C. § 142.

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.

Notice of Secret Service use of facial recognition technology is provided by the publication of this Privacy Impact Assessment and by the Field Investigative Reporting System Privacy Impact Assessment and its associated System of Records Notice (SORN).[16] Since a facial recognition technology is a law enforcement tool that the Secret Service Office of Investigations uses in furtherance of Secret Service criminal investigations, it may not be feasible to provide notice to individuals at the time their image is collected and submitted to or matched against images in a gallery. Some images may be collected through legal processes, such as subpoenas and search warrants, through which individuals are notified of the collection of their images.

Privacy Risk: There is a risk that individuals may not know that their image(s) may be used by Secret Service for facial recognition matching.

Mitigation: This risk is partially mitigated. Notice to individuals is provided through publication of this Privacy Impact Assessment and associated System of Records Notice. Secret Service Office of Investigations personnel may use only approved government agency facial recognition technology. The Office of Investigations Criminal Investigative Division, in consultation with the Secret Service Office of the Chief Counsel and Secret Service Privacy Office, is responsible for the facial recognition technology approval process, to include any further approval and safeguards required by DHS. It is incumbent on the Office of Investigations Criminal Investigative Division to ensure that facial recognition technology it uses provides sufficient notice that images collected and maintained by the agency may be used in facial recognition matching activities. Many government agencies use images collected for law enforcement purposes and background checks, such as mugshots and visa photos, for facial recognition purposes. These images are often collected directly from an individual and so they are notified directly that their image may be used for law enforcement purposes. Some government agencies, such as the Departments of Motor Vehicles in participating states, collect images for purposes unrelated to law enforcement, but notify individuals generally that information collected by them could be used for law enforcement purposes, including facial recognition matching. The Secret Service Office of Investigations does not control the notice provided by other government agencies to individuals at the time of collection and cannot notify an individual when Secret Service personnel use their image facial without risking informing a criminal suspect of an active investigation.

[16] *See* DHS/USSS-001 Criminal Investigation Information System of Records Document, 85 Fed. Reg. 64523 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

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 Secret Service Office of Investigations collects evidence, which includes photographs of alleged victims or suspects, during a criminal investigation in accordance with criminal procedure and DHS and Secret Service policies. The Secret Service Office of Investigations will use government agency facial recognition technology when an individual cannot be identified, or in some cases, when an individual's identity must be verified, in support of an open and authorized Secret Service investigation.

Secret Service Office of Investigations does not control the access and correction procedures for facial recognition technology maintained by other agencies. It is, however, responsible for providing access and correction mechanisms for the information it maintains and uses, as well as for any actions Secret Service may take based on facial matching completed by other agencies. Accordingly, Secret Service will notify other government agency of any misidentifications/false negatives/false positives, keep an accounting of these issues, and assess whether continued use of the other government agency's technology is appropriate.

The ability for an individual to opt out of facial recognition queries run by or to access and amend information in another agency's image gallery is entirely dependent upon the other government agency's processes. Mechanisms for access, correction, and redress regarding use of personally identifiable information in other federal government agency databases may be addressed within their relevant Privacy Impact Assessments and System of Records Notices. State Department of Motor Vehicle databases similarly allow, or require, individuals to correct and update information.

The Secret Service does not provide an opt out option for use of an individual's image for facial recognition purposes due to its law enforcement interests. Individuals seeking access to any record maintained by the Secret Service, or seeking to contest the accuracy of its content, may submit a Privacy Act (PA) request to the Secret Service. Individuals, regardless of citizenship or legal status, may also request access to their records under the Freedom of Information Act (FOIA). Access requests should be directed to the Secret Service FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223 or FOIA@usss.dhs.gov. Requests will be processed under both FOIA and the Privacy Act, as appropriate, to provide the requestor with all information that is releasable. Given the law enforcement nature of Secret Service use of facial recognition technology, all or some of the requested information may be

exempt from access pursuant to applicable exemptions, including those designed to prevent harm to law enforcement investigations or interests.

Notwithstanding the applicable exemptions, Secret Service reviews all such requests on a case-by-case basis. Instructions for filing a Freedom of Information Act or Privacy Act request are available at http://www.dhs.gov/foia.

Privacy Risk: There is a risk that individuals may not consent to Secret Service use of facial recognition technology, which can lead to their identification and Secret Service enforcement activity against them.

Mitigation: This risk is partially mitigated. Facial recognition technology that is maintained by federal, state, and local government agencies and used by Secret Service generally collects images for their galleries directly from individuals. During image collection these agencies also collect from the individual biographic information that will be associated with the image. This includes consensual collections, such as images for state identification or visa applications, or non-consensual collections, such as mugshots. An individual may have the opportunity in most instances of consensual collections to opt out of having themselves photographed. However, they may then forfeit the ability to use the service (licensure) or benefit (visa) for which they applied.

In addition, to ensure that facial recognition technology outputs are not used as the sole basis to identify individuals and engage in a law enforcement action, Secret Service Office of Investigations personnel use a facial recognition technology to generate candidate lists as investigative leads which require further measures to determine the identity of individuals contained on the candidate list. Additionally, prior to using a facial recognition technology, Secret Service Office of Investigations personnel must first make reasonable efforts to identify an individual through other existing means and methods, such as government database queries, open-source research, and other routine investigative techniques based on biographical and other non-biometric information.

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 Secret Service Office of Investigations is authorized to use facial recognition technology and related information under 18 U.S.C. § 3056, "Powers, Authorities, and Duties of United States Secret Service." The Secret Service Office of Investigations investigates cyber-enabled crimes, financial crimes, and counterfeiting. Secret Service Office of Investigations will only use facial recognition technology and associated information in furtherance of ongoing, authorized criminal investigations and submit probe images that are linked to ongoing criminal investigations for crimes Secret Service Office of Investigations has the statutory authority to

enforce. Secret Service Office of Investigations maintains probe images and results of facial recognition technology queries in the Secret Service Field Investigative Reporting System, and in accordance with the Privacy Act of 1974.[17]

Privacy Risk: There is a risk that Secret Service Office of Investigations may use a facial recognition technology for purposes beyond what is described in this Privacy Impact Assessment and permitted by DHS and Secret Service policy.

Mitigation: This risk is mitigated. Secret Service Office of Investigations has developed controls to audit use of facial recognition technology in support of Secret Service criminal investigations. These controls enable Secret Service Office of Investigations to capture information associated with facial recognition technology used in support of investigative activities to include: (1) the owner and/or operator of the facial recognition technology; (2) what facial recognition technology was used; (3) date the search was conducted; and (4) corroborative findings and identification results. The Secret Service Office of Investigations Criminal Investigative Division policy limits Secret Service Office of Investigations personnel to only use approved facial recognition technology maintained by other government agencies for ongoing, authorized Secret Service criminal investigations. The Secret Service Office of Investigations Criminal Investigative Division is responsible for meeting Secret Service requirements and completing the Department's facial recognition technology approval process, to include (1) independent testing and evaluation under the oversight of the Science and Technology Directorate (S&T), and (2) review and approval by the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, the Chief Information Security Officer, the Director of the United States Secret Service, and the Chief Information Officer.[18] Secret Service personnel are required to annually complete the information technology (IT) awareness training that provides IT rules of behavior and other applicable policy directives related to the handling and safeguarding of sensitive data, as well as annual privacy awareness training.

Secret Service Office of Investigations will incorporate reviewing the use of facial recognition technology by Secret Service Office of Investigations personnel in current quality assurance processes and audits applicable to Secret Service Office of Investigations case management and the Secret Service Field Investigative Reporting System.

[17] 5 U.S.C. § 552a.
[18] *See* DHS Instruction 026-11-001, USE OF FACE RECOGNITION AND FACE CAPTURE TECHNOLOGIES, *available at* https://www.dhs.gov/publication/information-and-technology-management.

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 Secret Service Office of Investigations has policies and oversight processes regarding evidence gathering and handling. The Secret Service Office of Investigations only collects information in furtherance of statutory law enforcement authorities for the purposes of furthering ongoing Secret Service investigations.

The Secret Service Office of Investigations may not create or use probe images from data collected from individuals actively exercising rights protected by the First Amendment to the United States Constitution (e.g., at religious services or political protests). Secret Service Office of Investigations will only create or use probe images of suspects or victims directly related to crimes Secret Service Office of Investigations is authorized to investigate.

Privacy Risk: There is a risk that use of facial recognition technology may return images of potential candidates not determined to be relevant to an ongoing investigation, leading to an overcollection by Secret Service of personally identifiable information irrelevant to the ongoing criminal case.

Mitigation: This risk is not mitigated. Facial recognition technology outputs return images of potential candidates that meet the established threshold/similarly score. This is why Secret Service requires its officers to attempt to identify a suspect or victim using means other than just facial recognition. As noted, facial recognition candidate lists are used by Secret Service to develop investigative leads, requiring corroboration with other information to identify leads; they may not be used as the sole basis for identity confirmation or enforcement action.

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: This risk is mitigated. The relevant Secret Service Office of Investigations investigative records retention schedule[19] is applicable to the retention and disposition of the investigative case file and the associated probe images and candidate lists maintained therein. Retention and disposition of biometric records and their associated biographical data are governed by DHS Records Control Schedule DAA-0563-2013-0001, which was approved by the National Archives and Records Administration (NARA). Secret Service ensures proper disposition through technical and manual controls and audits.

[19] See, e.g., NC1-087-84-01, N1-087-89-002, and NC1-087-92-02. Note, these schedules have been consolidated and are currently pending final NARA approval/issuance under a new schedule number, DAA-0087-2021-0001.

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.

The Secret Service Office of Investigations will only use and share probe images for the purposes for which they were obtained as outlined in this Privacy Impact Assessment and the applicable System of Records Notice, which is to conduct authorized Secret Service criminal investigations. The Secret Service Office of Investigations limits the use of facial recognition technology to ongoing, authorized investigations. The Secret Service Office of Investigations does not use facial recognition technology to surveil the public, nor does it use commercially provided services. The Secret Service Office of Investigations does not have the capability and will not procure any device that uses facial recognition technology to analyze live video, streaming media, or any other media in real-time. External sharing involves use of a probe image for facial recognition purposes using another government agency's technology, in furtherance of a Secret Service criminal investigation. The other government agencies are not permitted to retain the probe images used by Secret Service.

Privacy Risk: There is a risk that the Secret Service Office of Investigations may use probe images for facial recognition purposes that are not directly relevant to an ongoing criminal case.

Mitigation: This risk is partially mitigated. The Secret Service Office of Investigations policy details the approval process for use of facial recognition technology and the appropriate uses of existing facial recognition technology. The Secret Service Office of Investigations policy mandates that Secret Service Office of Investigations personnel may only use facial recognition technology to submit probe images for identification of potential matches to investigative subjects and victims in ongoing Secret Service criminal investigations for crimes the Secret Service has statutory authority to enforce. Secret Service Office of Investigations personnel may only use other government agency facial recognition technology that is approved by the Secret Service Office of Investigations Criminal Investigative Division. Secret Service Office of Investigations personnel that violate DHS and/or Secret Service policy, to include mishandling probe images, may be subject to disciplinary action by Secret Service through established processes.

Privacy Risk: There is a risk that other government agencies may retain and use probe images submitted by the Secret Service Office of Investigations for purposes other than use as a probe image by Secret Service.

Mitigation: This risk is mitigated. Secret Service probe images may not be retained or used by the other government agencies. The probe image may only be used to facilitate a facial recognition technology query by another government agency on behalf of and in support an open and authorized Secret Service investigation.

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.

Due to the potential for facial recognition technology to produce false positive/false negative matches, the Secret Service Office of Investigations only uses facial recognition technology as a step in an investigative process: to generate potential leads. Outputs of facial recognition technology can vary on a case-by-case basis. This is because the accuracy of an algorithm and/or input data (i.e., probe images) used for facial recognition varies.

Accordingly, Secret Service Office of Investigations policy requires that all candidate returns may be used for lead purposes only, and may not be used on their own to positively identify individuals or engaged in enforcement actions. The Secret Service Office of Investigations personnel must compare and corroborate candidate returns through non-biometric investigative processes. Candidate returns may not be considered an indicator of unlawful activity and may not be used on their own to establish probable cause. If a lead is created because of a vetted match, it must then be combined with other relevant and credible evidence to establish probable cause.

Privacy Risk: There is a risk that Secret Service may submit low quality probe images that could increase the likelihood of false positive matches.

Mitigation: This risk is partially mitigated. Secret Service Office of Investigations personnel are trained on proper collection and isolation techniques (e.g., zooming, cropping) to reduce variations between a probe photo and an image gallery. As the biometric service provider, the other government agency also may reject a probe image that is too low quality to produce a candidate list within the designated threshold.

Privacy Risk: There is a risk that a facial recognition technology will misidentify individuals leading to incorrect enforcement actions by Secret Service.

Mitigation: This risk is mitigated. Use of facial recognition technology by Secret Service Office of Investigations personnel is limited to using candidate lists for lead purposes only (e.g., for further investigation), and may not be used as positive identification of an individual or as the sole basis for an enforcement action. Secret Service Office of Investigations personnel must vet individuals on a candidate list by using other corroborating information.

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.

Secret Service Office of Investigations personnel authorized to use facial recognition are responsible for the security of personally identifiable information transmitted and received. Secret Service Office of Investigations personnel follow DHS and Secret Service policies and procedures on safeguarding personally identifiable information and sensitive personally identifiable information. Secret Service Office of Investigations personnel are required by policy to ensure that transmission and receipt of personally identifiable information are appropriately encrypted in accordance with DHS standard operating procedures in the safeguarding of sensitive personally identifiable information, governing information sharing agreements,[20] and Secret Service standards on the handling of law enforcement sensitive information. In addition, Secret Service Office of Investigations personnel may only use other government agency approved facial recognition technology. The Secret Service Office of Investigations Criminal Investigative Division, in consultation with the Secret Service Office of the Chief Counsel and Secret Service Privacy Office, is responsible for the facial recognition technology approval process, to include any further approval and safeguards required by DHS. In addition to compliance with DHS directives, the approval process requires the evaluation of the facial recognition technology to ensure that methods of transmission of the probe image are properly encrypted, the facial recognition technology has the appropriate safeguards for housing sensitive personally identifiable information, and the facial recognition technology does not retain or re-disseminate Secret Service Office of Investigations probe images. Internally, Secret Service Office of Investigations minimizes the privacy impacts of using facial recognition technology through safeguards similar to those used for Secret Service use of other personally identifiable information, sensitive personally identifiable information, and law enforcement sensitive information collected and maintained in furtherance of criminal investigations.

Privacy Risk: There is a risk that a facial recognition technology will mishandle Secret Service Office of Investigations data, leading to a data breach or privacy incident.

Mitigation: This risk is partially mitigated. Secret Service Office of Investigations personnel may only use approved facial recognition technology. The Secret Service Office of Investigations Criminal Investigative Division, in consultation with the Office of the Chief Counsel and the Privacy Office, is responsible for the facial recognition technology approval

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSITIVE PII (2017), *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

process, to include any further approval and safeguards required by DHS. In addition to compliance with DHS directives, the approval process requires the evaluation to ensure that methods of transmission of the probe image are properly encrypted and the other government agency follows appropriate safeguards for protecting sensitive personally identifiable information.

The Secret Service Office of Investigations will incorporate reviewing the use of facial recognition technology by Secret Service Office of Investigations personnel in quality assurance processes and audits applicable to Secret Service Office of Investigations case management and the Secret Service Field Investigative Reporting System.

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.

Information used and collected through use of facial recognition technology, and the corresponding vetting and investigation process, will be documented in the relevant investigative case file in the Secret Service Field Investigative Reporting System consistent with Secret Service Office of Investigations policy and federal law.

Secret Service Office of Investigation's use of facial recognition technology is an extension of its existing investigative processes. Therefore, the auditing and oversight of use of facial recognition technology is consistent with the handling of information maintained in the Secret Service Field Investigative Reporting System. Candidate returns and any leads generated will also be recorded in the Secret Service Field Investigative Reporting System. As such, accountability checks regarding the collection, sharing, and receiving of information in connection with use of facial recognition technology is dependent on Secret Service Office of Investigations personnel following Office of Investigations standard procedures and requirements for logging information in the Secret Service Field Investigative Reporting System. The Secret Service Office of Investigations also has existing policies and oversight processes regarding evidence gathering and handling, subject to Secret Service audits and compliance inspections.

Conclusion

Facial recognition is a rapidly developing capability. Secret Service Office of Investigation's use of this technology is to help identify criminals engaged in cyber-enabled crimes, financial crimes, and counterfeiting. While the technology and the Secret Service's use of the technology and its output have privacy implications, Secret Service Office of Investigations has established processes and procedures to mitigate the impact of using facial recognition technology in support of its authorized investigations. Through proper collection, handling, review, maintenance procedures, candidate vetting, and supervisory oversight of investigative

activities, Secret Service Office of Investigations will utilize facial recognition technology in a privacy preserving manner.

Contact Official

Christal Bramson
Privacy Officer
U.S. Secret Service
privacy@usss.dhs.gov

Responsible Official

Brian S. Lambert
Assistant Director
U.S. Secret Service
Office of Investigations

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Deborah Fleischaker
Acting Chief Privacy Officer
U.S. Department of Homeland Security
privacy@hq.dhs.gov