Privacy Impact Assessment
for the

ICE Use of Facial Recognition Services

DHS/ICE/PIA-054

May 13, 2020

<u>Contact Point</u>
Alysa D. Erichs
Acting Executive Associate Director, Homeland Security Investigations
U.S. Immigration & Customs Enforcement
Department of Homeland Security
(202) 732-5100

<u>Reviewing Official</u>
Dena Kozanas
Chief Privacy Officer Department of Homeland Security
(202) 343-1717

Abstract

Homeland Security Investigations (HSI) is the investigative arm of U.S. Immigration and Customs Enforcement (ICE) and is focused on countering domestic and transnational crimes. In the course of its investigations, HSI routinely encounters digital images of potential victims or individuals suspected of crimes but cannot connect those images to identifiable information through existing investigative means and methods. HSI, therefore, submits those images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes. The agencies and vendors query their databases for potential matches and return lists of potential candidate matches that HSI can use to produce investigative leads. HSI is conducting this Privacy Impact Assessment (PIA) because the use of these facial recognition services (FRS) requires the collection, maintenance, and use of personally identifiable information (PII).

Introduction

Facial Recognition Technology

Developments in machine learning, artificial intelligence (AI), and cloud technologies have drastically increased the speed and efficiency at which large volumes of data can be processed. These developments have enabled advances in face-based biometric identification called facial recognition. Facial recognition technology uses an AI algorithm to analyze human faces captured in photo or video footage. The facial recognition AI identifies facial landmarks such as eyes, bone structure, lips, nose, and mouth to generate a facial measurement, and compares the generated measurement to those already in the database to search for a potential match.

Facial recognition tools improve by training the AI through a process called machine learning. Facial recognition developers create a program that recognizes landmarks within a face, such as the tip of a nose or the center of an eye, and then calculates the distances between those landmarks. The program saves these calculations in a template, which is represented as a sequence of characters and numbers. Each template is unique to the program that created it and cannot be reverse engineered to re-create the submitted image. During the training process, the facial recognition program will compare each template to a set of training images annotated by the AI's developers. The program makes a hypothesis about the similarities between the two images, and the developers then confirm whether the hypothesis was correct. Through this process, the AI gradually learns what makes two images similar or different from each other. As noted in the

Accuracy Rates section below, there are widely accepted scientific processes to confirm that a facial recognition program is functioning reliably and accurately.[1]

When developers have determined an AI has consistently and successfully matched images, it can then be used to compare a submitted image to images on file. The facial recognition technology can be used to verify that an individual in a submitted image is the same individual depicted in a facial verification (a 1:1 match), image comparison (2-photo submission) or to identify an unknown individual by querying an entire gallery of images in a database to find an image similar to a submitted image (1:many match or identify candidates). Facial recognition algorithms are developed for particular uses by their developers and an algorithm's accuracy, functionality, or use cases will be highly contextual. For example, some facial recognition technologies are used in mobile phones and cameras to detect faces in a photograph but are not accurate enough to identify an individual. Similarly, a facial recognition technology employed by a phone manufacturer may be accurate enough to provide access to that phone but would not be reliably accurate to use in a law enforcement context.

As with any AI application, the accuracy of a facial recognition algorithm directly correlates with the breadth and quality of the data on which it is trained. Contextual factors may include the demographic of the population, camera quality, the rate of throughput, lighting, distance, and size of the database, as well as other factors.

Facial recognition algorithms must be trained with a diverse population of images to minimize misidentifications across all demographics of the population (e.g., age, gender, race). If developers have a large and diverse pool of training data, these programs are then more likely to create accurate hypotheses across races, ethnicities, and ages.[2]

Additionally, as a comparison tool, facial recognition operates with greater accuracy when there are fewer variables between pictures. This often requires ensuring that lighting conditions in the submitted image are similar to those in which the compared images were taken. Additionally, angles or distances between a subject and a camera should be similar. "Constraining" an image reduces variables by requiring that similar poses, expressions, lighting, and distances be adopted across images. Common examples of constrained images are mugshots and visa photographs. Photographs that are unconstrained, or taken "in the wild," such as images derived from surveillance activities or pulled from social media, are at a greater risk for inaccurate matches.[3]

Moreover, facial expressions, aging, and the obscuration of an individual's face by glasses, hats, and facial hair can further reduce the effectiveness of facial recognition. For this reason, the

[1] For more information *see* https://fiswg.org/index.htm.

[2] For more information *see* NIST, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (Dec. 2019) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[3] For more information *see* NIST, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" pg. 5. (Nov 2018) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

effectiveness of using facial recognition on an unconstrained image may vary based on seasonality (e.g., lower light levels and more individuals wearing hats or scarves in winter) or regional and cultural norms. Recognizing this factor, some FRSs have worked to create specialized algorithms that perform better on unconstrained facial images. While tending to be significantly slower and requiring computational resources than algorithmic models focused on constrained facial images, these FRSs provide greater accuracy when comparing unconstrained images.

Accuracy Rates

Accuracy rates are measures of the algorithms' efficacy by either the AI developers or an outside validator, such as the National Institute for Science and Technology (NIST). Accuracy rates are measured by how often the AI made the wrong hypothesis. An algorithm can be wrong in one of two ways: either guessing that images of two different individuals are the same person (false positive or false match) or guessing that two images of the same individual were not the same person (false negative or false non-match). While false non-match rates lower the efficacy of a facial recognition technology for HSI investigations, an algorithm's false-match rate has the greatest impact on individual privacy. ICE is working with the DHS Directorate of Science and Technology (S&T) on establishing an image quality capture standard to ensure consistency in data definition and accuracy for its use of facial recognition services.

Similarity Scores/Confidence Levels

A similarity score, sometimes known as confidence level, is a measure by the algorithm for how alike two compared images may be. A similarity score is different than an accuracy rate. Similarity scores are the statistical probability determined by the algorithm that an individual in a returned image is the same individual as the one in a submitted photo.[4] Similarity scores can be used as a threshold and are adjustable by a user. Setting a low similarity score threshold allows the algorithm to return larger sets of images from its gallery but increases the number of individuals who are likely not matches to the submitted image. For example, a similarity score set at a threshold of 85 will return all images that have an 85% or greater likelihood to be the same individual as one whose image has been submitted for identification. The algorithm generates a list of potential candidates, one of whom may match the submitted image. The user reviews the candidate list to determine if there is a successful match. In instances where a technology returns a list of candidates instead of an individual the facial recognition technology will always have a 100% error rate (deemed a false match rate), in that it will always return individuals who are not the individual depicted in the submitted image. The larger candidate lists, however, reduce disparate impacts of inaccuracy in the technology since it becomes more likely the correct

[4] McLaughlin, Michael & Castro, Daniel, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist" (Jan 2020) *available at* https://itif.org/sites/default/files/2020-best-facial-recognition.pdf.

individual is in a return and reduces the persuasiveness of an algorithmic return by showing multiple individuals that may share different biometric traits.[5] For example, an individual may share the same eye features with one individual, but the same nose landmarks as a different individual. As candidate list sizes grow, so does the amount of shared biometric traits across the return. The candidate list then becomes less certain. Candidate lists of any size require the user to complete additional steps (manual examination of the images or further investigation) to verify a match.

Candidate returns can also be set by a pre-determined list size. In these instances, the facial recognition service could return the number of most likely matches in the gallery, regardless of the statistical likelihood any will match. There is also the possibility that a service allows a user to set both a confidence threshold and list size. For example, a user may request a candidate list of 20 individuals with highest similarity scores unless a candidate's score is below 50%. This allows for the service to return large candidate lists, but reduces the likelihood of returning irrelevant candidates to a user. HSI will opt for a candidate list when using an FRS, and if possible, choose a candidate list length that is considered as best practices by law enforcement at the time of the query (e.g., 20 candidates) unless mission needs require a different number.

Facial Recognition Services

This PIA will focus on HSI's use of facial recognition services (FRS).[6] An FRS is a government agency or commercial vendor managing its own image databases and choosing its own facial recognition technology. Those agencies and vendors accept facial images from third parties, including HSI, to run comparative queries of its own image galleries using its own facial recognition algorithm. Examples of the types of FRS's that HSI uses are listed below.[7]

HSI uses an FRS's 1:many query functionalities to generate candidate lists to identify an unknown person or to locate a known person who may be using an alias or assumed identity. These requests are made in furtherance of ongoing investigations on a case-by-case basis.[8] ICE HSI

[5] For more information *see* NIST, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" (Nov 2018) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

[6] This PIA does not contemplate HSI owning or operating an algorithmic matching technology to run image searches against its own database. Within the Victim Identification (VID) Program algorithmic image matching is used to manage the National Child Victim Identification System 2 (NCVIS2), which is HSI's repository for all images and videos related to child exploitation material. No other PII is associated with images in NCVIS2 and the process is used to link cases. For more information *see* DHS/ICE/PIA-010 NCVIS *available at* www.dhs.gov/privacy. Any future acquisition or development of a facial recognition program by ICE will be covered in a separate PIA.

[7] *See* "Types of Facial Recognition Services used by HSI" section.

[8] This pertains to HSI making requests to FRSs, and not automated multi-modal biometric queries that may occur upon the enrollment of an individual in a biometric database. Further, this does not pertain to partner agencies running facial recognition queries as part of their own processes in a joint investigation in which HSI may be a partner.

primarily uses this law enforcement tool to identify victims of child exploitation and human trafficking, subjects engaged in the online and sexual exploitation of children, subjects engaged in financial fraud schemes, identity and benefit fraud, and those identified as members of transnational criminal organizations. HSI minimizes the privacy impacts of using an FRS through safeguards it has instituted at each step of the identification process. This process includes the initial collection of probe photos,[9] the submission of probe photos to the FRS, and the receipt and use of candidate lists from an FRS. Further, HSI does not take enforcement action against any individual solely based on candidate images. Rather, HSI uses these candidate images as leads, which always requires further corroboration and investigation.

Collection of Probe Photos

ICE uses an FRS by submitting facial images called probe photos. Probe photos must be directly relevant to an investigation and are only submitted to an FRS to further an active investigation. HSI collects a range of photographs during routine investigative activity including mugshots, surveillance photos, social media posts, and images confiscated from phones or other data devices. HSI may also isolate still frames from videos or streaming media to create a probe photo. Any of these sources can be used to isolate a facial image and create a probe photo.

HSI may collect constrained images and use an FRS to verify the asserted identity of an individual in limited circumstances, such as in suspected identity fraud cases. For example, HSI may submit a passport photo to an FRS to determine if that individual is linked to other names/identities held by that FRS.

The majority of images collected by HSI will be "unconstrained." Unconstrained images, often derived from surveillance activities or pulled from social media, inherently do not have the same controls on variation as constrained images. Some variations, however, can be reduced when the HSI agent collects/chooses the photo and isolates the facial image from the photo. The HSI agent will select isolated images that are best suited to be probe photos for the facial recognition processes. The HSI agent will ensure he or she isolates the facial image with the highest image quality possible, containing the fewest obstructions to the subject's face, and is most similar to a constrained image with regard to variables such as angle, lighting, distance, and subject expression. HSI endeavors to isolate images as similar as possible to those maintained in the galleries of an FRS (such as mugshots or passport photographs) to increase the likelihood of accuracy.

HSI safeguards prior to using Facial Recognition Services

Prior to submitting an image to an FRS, the HSI agent assigned to the case must first make reasonable efforts to identify the individual through existing means and methods. The agent must use reasonable efforts to identify the individual through government database queries, open source

[9] Probe photos are facial images that are lawfully obtained pursuant to an authorized criminal investigation and submitted for facial recognition matching.

research, and other conventional investigative techniques based on biographical and other non-biometric information prior to submitting a probe photo to an FRS. The agent's use of existing processes must be noted in the ICE Investigative Case Management System (ICM)[10] as a Report of Investigation (ROI). This documentation may occur after a query is conducted but must be completed prior to generating any lead for further investigation (see below).

HSI agents may only use an approved FRS for facial recognition identification. The approval process for an FRS can either be accomplished on a case-by-case basis at the HSI supervisor level or an FRS can be approved for HSI-wide use by the HSI Operational Systems Development and Management unit (OSDM). The mission of the OSDM is to coordinate development of new information technology (IT) systems, maintain existing IT systems, and identify new technologies for HSI. An HSI agent may submit an FRS to OSDM for inclusion onto a list of approved FRSs. OSDM will then evaluate the FRS to ensure that methods of transmission of the probe photo are properly encrypted, the FRS has the appropriate safeguards for housing sensitive PII, and the FRS does not retain or re-disseminate HSI probe photos. OSDM will consult with ICE Privacy, ICE attorneys, and other stakeholders throughout the evaluation process. OSDM will leverage resources such as NIST's Face Recognition Vendor Test (FRVT)[11] to evaluate the accuracy and bias of an FRS. Additionally, OSDM will conduct non-scientific tests of the FRS to gain insight into the veracity of the service. These evaluations will be necessary for approval by OSDM, but will not add weight to an FRS's returns. All returns will only be treated as investigative leads by HSI.

If an FRS is not pre-approved by OSDM and exigent circumstances dictate that the FRS must be used prior to OSDM review, the HSI agent must seek HSI supervisor approval prior to sending a probe photo. The HSI supervisor will confirm the exigent circumstance and ensure that the FRS is relevant and necessary for the investigation. The HSI supervisor will then submit the FRS to OSDM for review. The HSI supervisor will not evaluate an FRS's algorithm for accuracy or bias, as he or she does not have the technical capacity to comprehensively assess facial recognition technologies. OSDM will conduct a review of the FRS that was used and will ensure that the probe photo was not retained or reused by the FRS outside of the HSI-requested query.

When the HSI agent submits the probe photo, the agent notes the agency or vendor providing the FRS as part of the ROI in ICM. HSI supervisors are required to perform a review of agent submissions to FRS's on a periodic basis. HSI supervisors review ICM and the relevant case file to ensure agents use FRS's by the terms outlined in this PIA.

[10] *See* DHS/ICE/PIA-045 Investigative Case Management System (ICM) *available at* www.dhs.gov/privacy.

[11] For more information *see* https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

Submission Process to a Facial Recognition Service

HSI uses FRS databases that are open to federal law enforcement. Each FRS is entirely overseen and operated by the agencies and vendors that possesses the image galleries. HSI agents will either submit the probe photo manually to the FRS (e.g., via encrypted email) and a representative of the FRS will then input the image into their database to use the facial recognition technology, or will upload the photo directly to the FRS via a web interface.

HSI, through the Repository for Analytics in a Virtualized Environment (RAVEn) system,[12] will also develop a connection with OSDM-approved FRSs for HSI agents to submit probe photos. This will allow HSI to format probe photo submissions to the American National Standards Institute (ANSI)/NIST Type 10 record format for data exchange,[13] as well as to log and track all submissions by HSI and all returns by FRSs to ensure adequate security of the data and oversight of the use of FRSs. When this capability is developed, ICE Privacy will note the functionality in an update to the RAVEn PIA appendices.

HSI will only supply the minimum information required by the FRS to run the query. Usually this will only be the case agent's information and the probe photo itself. Some government FRSs may require the statutory authority or suspected crime to be submitted as well. For purposes of individual privacy and investigative case integrity, HSI will refrain from submitting more data than needed to the FRS.

In instances in which HSI may need a facial recognition service to verify the claimed identity of an individual during an investigation, HSI will request a 1:many query, as opposed to 1:1 verification. As discussed below, the impact of inaccuracies or biases in an FRS algorithm is reduced by returning a candidate list instead of a positive identification.

For instances like identity fraud, in which HSI requires facial recognition processes to assist with facial image comparison (2-image submission), HSI will only submit probe photos to an OSDM-approved FRS.[14] The submission and receipt process will be similar to a 1:many query request, but HSI will instead receive only a similarity score of the two photos from the FRS. For example, HSI may ask an FRS to determine the likelihood that an image in a passport photo matches the image in a photograph taken during the course of a law enforcement investigation. No PII will be returned as an output of an image comparison. The HSI agent may, if needed, submit a request to a relevant and necessary FRS for leads to the actual identity of an individual.

[12] *See* DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment (RAVEn) *available at* www.dhs.gov/privacy.

[13] ANSI/NIST ITL 1-2011, Update 2015, Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, https://www.nist.gov/programs-projects/ansinist-itl-standard.

[14] *See* "Types of Facial Recognition Services" section below.

For a 1:many identity query HSI will only submit probe photos to an FRS whose query will not result in a single identity match, but rather in a candidate list of potential matches, which may be ranked by similarity scores.

This process generally works as follows:

- An HSI agent will come into possession of a facial image through existing investigative means and methods (e.g., via surveillance photographs, subpoenaed records, or identity documents); the image could be of individuals victimized by or suspected of committing a crime ICE has the legal authority to investigate.
- The HSI agent determines that use of the FRS is approved by HSI OSDM, is necessary, and is reasonably likely to result in a positive identification.
- If the FRS has not been previously approved, an HSI supervisor must approve the use of the FRS after ensuring that the circumstances require immediate submission to the FRS, and that the FRS will in turn be submitted to OSDM for further review as circumstances permit.
- If an FRS is approved, the HSI agent would submit the probe photo to the facial recognition service under the terms of service required by that agency or vendor and note the use of the FRS in ICM.
- The FRS will run a 1:many matching algorithm, by which it will compare the probe photo against its current galleries (e.g., mugshots and drivers' license records).
- The FRS will return a candidate list to the agent that may contain the similarity scores of each candidate. The candidate list may also contain any associated biographic information about a candidate currently contained within the FRS's database. The type of information will vary depending on the database (e.g., a law enforcement database may have derogatory information while a state Department of Motor Vehicles (DMV) database has driver records).

Some FRSs provide requestors the option of having their candidate lists reviewed by trained biometric face examiners. Face examination and reporting processes are based on best practices established by the Facial Identification Scientific Working Group (FISWG),[15] which operates under the NIST-run Organization of Scientific Area Committees (OSAC) for Forensic Science. The examiners will review algorithmic candidate returns using analysis of unique facial features called "morphological analysis."[16] In these instances the FRS technology will still provide a multiple candidate return, but the facial examiners provide an interim step of manual biometric

[15] For more information *see* https://fiswg.org/about_swgs.html.

[16] *See* FISWG Best Practices for Facial Image Comparison Feature List for Morphological Analysis, *available at* https://www.fiswg.org/FISWG_GuidelinesforFacialComparisonMethods_v1.0_2012_02_02.pdf.

analysis according to established industry standards and practices promulgated by the FISWG. If the FRS provides this option to HSI, then HSI may opt for the additional manual review. If HSI chooses to have returns analyzed, the examiner will provide HSI a narrowed candidate list, which may be as small as one individual. The examiner will also supply a confidence level score for each image returned, which is the examiner's explanation of the likelihood of a match between analyzed images. Manual facial examination by an FRS facial examiner is only a narrowing tool. It does not change the process by which HSI receives or uses returned images and does not provide add certainty that a match is contained in a candidate list that is returned.

Receipt and use of FRS Candidate lists for Lead Generation

Upon receipt of the candidate list, the HSI agent will compare the information returned by the FRS to other biographical and derogatory information in open source systems and governmental databases to determine if any matches are supported by corroborating evidence. This process is known as "vetting." HSI agents will not attempt to act as biometric face examiners and will instead compare candidate returns through non-biometric investigative processes. FRS similarity scores, if provided, will only be used as a triage tool for HSI vetting, not as an indicator of any criminal activity. To reduce any impacts caused by algorithmic inaccuracy or bias, HSI will not use an FRS return for 1:many queries that does not have a list of multiple candidates. If a multiple candidate return is narrowed to one individual by the FRS face examiner, HSI will still not consider the return a positive identification and will still vet the individual returned through open source systems and governmental databases. Similarly, HSI will only use an OSDM-approved FRS for 2-image photo comparison because the technology's accuracy and biases are continuously vetted by ICE subject matter experts.

An HSI agent will compare information received from an FRS to other information available to HSI from various sources to vet the potential match. Additional evidence leading to validation or elimination of a candidate as a possible match could include: biographic information, current and previous addresses, telephone numbers, vehicles, criminal history, immigration history, and information derived from publicly available social media. Candidate lists will be maintained in an external investigative case file as required under the Federal Rules of Evidence, or any other applicable statute, regulation or policy,[17] but non-vetted candidate information will not be used for leads or entered in an ROI in ICE systems and cannot be queried by ICM or other ICE systems.

If a candidate returned from the FRS is successfully vetted, the HSI agent will work up a lead for further investigation. Any lead related to a case is entered into ICM as a Report of Investigation (ROI). The fact that a lead was derived from an FRS generated candidate list will also be noted in the ROI, including the name of the FRS (e.g., name of the state DMV, name of

[17] *See* https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.

the commercial vendor source). HSI submits probe photos to FRSs for the purposes of establishing investigative leads. Leads are information with varying levels of credibility and will never be the sole basis used to establish probable cause, determine wrongdoing, or deny a benefit. FRS returns are generally accompanied by a disclaimer reminding the recipient that FRS processes are for lead generation purposes only and do not produce a product of sufficient weight to be used solely for a law enforcement action. For example, DHS's Office of Biometric Identity Management (OBIM) FRS returns the following disclaimer:

"OBIM Disclaimer: 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."

These disclaimers are produced by all federal FRSs used by HSI and ICE Privacy is required to screen new procurements before ICE purchases a commercial vendor FRS license. HSI will endeavor to ensure an FRS includes a disclaimer with a return prior to use, but if a candidate return is not accompanied by the disclaimer, HSI policy is to still treat all FRS returns as leads only.

Leads are only a first step in an investigative process of identification. Leads can come from any source and have varying levels of credibility. HSI agents routinely deal with leads during their day-to-day operations and are trained to validate or disprove leads through existing investigative methods. As an example, HSI operates a tip line to generate leads that averages 15,000 calls a month.[18] Similar to receiving a tip line lead, HSI agents are instructed that any vetted FRS candidate match must be further investigated by the HSI agent receiving the lead prior to ICE taking any enforcement action against an individual.

HSI agents who use an FRS must be able to testify to the use of facial recognition capabilities as other agents routinely testify regarding other biometric collection methods. HSI is developing, in consultation with ICE Privacy and S&T, a training on the processes and efficacy of facial recognition. If a lead is created from a vetted match and is then combined with other evidence to create probable cause, an agent may be required to testify to his/her use of an FRS in a judicial or administrative court. The HSI agent will also use such information in affidavits for warrants to explain how an agent initially identified a subject. A judicial court would then review the affidavit to ensure the veracity of the information prior to issuing the warrant. If a case is brought to trial,

[18] The HSI Tip line Unit is a 24-hour, seven days a week operations center. The Unit supports ICE's intake of and response to reports of suspicious activity or suspected illegal activity made by members of the public and other law enforcement agencies. For more information *see* DHS/ICE/PIA-033 FALCON Tipline *available at* www.dhs.gov/privacy.

information related to HSI's use of the FRS would be discoverable pursuant to normal judicial procedures.

Types of Facial Recognition Services used by HSI

FRSs are generally capabilities that were added to pre-existing biometric databases or criminal justice systems. The relevance of any particular FRS to an HSI investigation could be dependent upon the geographic location of the investigation, the type of investigation being conducted by HSI, and the type of image gallery the FRS contains. For example, an HSI agent would not submit a probe photo to an FRS run by a local police department in Florida if the crime being investigated took place in the state of New York, unless evidence or mission need dictated otherwise. Similarly, an HSI agent would be directed to first submit probe photos to the Department of State (DoS) Consular Consolidated Database (CCD) to determine if a passport or visa was fraudulent. Below are examples of the types of FRSs used by HSI. The list of FRSs is not exhaustive but will be updated in a PIA update if HSI uses an FRS of a significantly different type.

State and Local Facial Recognition Services

Many state and local law enforcement agencies (LEAs) throughout the United States have large databases of images collected during law enforcement actions (i.e., mugshots). Some of these agencies also connect directly to their associated DMV databases to allow for biometric querying of DMV information. It is common practice within the law enforcement community for LEAs to share information or allow other LEAs to submit biographic, descriptive, or other information in order to query their system. Many LEAs have now developed a service allowing external LEAs to submit probe photos to generate candidate lists from their databases for identification.

These state and local LEAs are geographically based and contain information collected within a particular locality. HSI would only submit probe photos to a state or local LEA if the agent had reason to believe the subject of the photo lived, visited, or had some other connection to that geographic location. The submission process for probe photos will vary by each LEA but generally follows the same process by which an HSI agent may request a biographic check for the subject of an investigation. Some states have granted HSI offices within their regions access to submit probe photos directly to the FRS. OSDM will review the terms and conditions of a new state or local FRS to ensure proper handling and safeguarding of HSI images. This will occur prior to submission of probe photos, except if an exigent circumstance requires immediate submission, then OSDM will review the terms and conditions as soon as possible thereafter. Regardless of the circumstances, any HSI user who wishes to access a state or local FRS must sign the FRS terms and conditions of service prior to accessing the service.

The number of candidates returned from a LEA FRS will vary as well as the type of biographic information returned with the list. If a LEA only queries a criminal database, then biographic and derogatory information would be returned to HSI. If the LEA connects to a state

DMV database, then a candidate's associated driver's license information could be included and driving records could also be accessed by HSI upon request.

Regional and subject matter-specific intelligence fusion centers

Transnational crime and criminal organizations expand beyond local or state jurisdictions. As such, many law enforcement agencies have partnered to create intelligence sharing centers (also called fusion centers) to collaborate and deconflict law enforcement activities regarding specific crimes (e.g., drug trafficking, human trafficking).[19] Fusion centers act as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal, territorial, federal, and private sector partners. HSI is a partner in many fusion centers whose mission aligns with HSI's statutory authorities so that HSI can track criminal activities, including those involving gangs, reported within a region.

Certain fusion centers have data analytic capabilities that aid investigators in processing and visualizing evidence. One capability that certain fusion centers are developing is an FRS to query their subject-specific galleries. Fusion center users can submit a range of photographs collected during law enforcement activities. This results in a repository of individuals identified as suspected of participating in a criminal organization for later use by the fusion center. The galleries are narrowly focused and directly relevant to HSI's queries.

If ICE is a partner in the fusion center, then HSI agents can submit probe photos of suspects. The center's FRS will run a matching algorithm that will compare the probe photo to its current gallery of known or suspected criminals. The FRS will return a candidate list from the gallery to the agent with a similarity score indicating the likelihood of identification to the probe photo.

The candidate lists will contain any information about a candidate that is currently contained within the fusion center. This could include biographic information, derogatory information, criminal intelligence, and known associates. Any information or connections made between submitted photos and entities within the fusion center must be manually entered by a fusion center user.

Federal Agency Facial Recognition Services

DHS Office of Biometric Identity Management (OBIM) Facial Recognition Services

OBIM's authoritative biometric database, the Automated Biometric Identification System (IDENT), is the central DHS-wide system for the storage and processing of biometric data.[20] This will change as OBIM completes its modernization by deploying the Homeland Advanced

[19] https://www.dhs.gov/fusion-centers.

[20] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

Recognition Technology (HART) system.[21] IDENT/HART stores and processes biometric data—digital fingerprints, facial images (photographs), and iris scans—and links biometrics with biographic information to establish and verify identities. OBIM serves as a biographic and biometric repository for all of DHS.[22] OBIM is in the process of connecting to FBI's Next Generation Identification (NGI) System, the Department of Defense's Automated Biometric Identification System (ABIS), and the Department of State's Consolidated Consular Database to enable requests for facial recognition queries through IDENT/HART.[23] OBIM identifies each collection by data provider and its authority to use, retain, and share data. IDENT 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. HSI agents may submit probe photos to IDENT/HART manually through OBIM's Biometric Support Center (BSC) or through a submission portal that is being developed on HSI's RAVEn platform. HSI will ensure that the BSC will delete probe photos after a query has been processed.

The output of an OBIM 1:many face query is a candidate list (a rank ordered list of the highest scoring comparisons above a preset threshold) of those images that data owners have permitted to be shared for this purpose. The length of the candidate list is selected by HSI. HSI will choose a list length that is considered best practice by law enforcement. HSI agents can access from an OBIM FRS query: biometric data; personal information (names, dates of birth, gender, etc.); personal identifiers (e.g., Alien number, Social Security number); biometric administrative identifiers (Federal Bureau of Investigation (FBI) Fingerprint Number -Universal Control Number (UCN), IDENT Fingerprint Identification Number (FIN), Department of Defense (DoD) Biometric Identity Number (BID)); personal physical details (e.g., height, weight, eye color, and hair color); identifiers for citizenship and nationality; derogatory information, if applicable; contact information; and encounter data.

Prior to HSI receiving the candidate list, the HSI agent can request the OBIM BSC provide examination. Trained BSC face examiners closely compare the probe photo against each of the candidate face images to determine if any of them are the same individual. Once results are verified, the BSC returns either a no-match or only those candidate(s) assessed to be likely matches. The return of a likely match will not be noted in IDENT/HART. If HSI validates a

[21] The migration from IDENT to HART operations occurs in phases to minimize impact to OBIM's mission partners. The migration will occur without unscheduled interruption of service delivery to OBIM's mission partners, with minimal scheduled service outages, and without degradation in service levels (response time) to those partners.

[22] *See* DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1 PIA, *available at* www.dhs.gov/privacy.

[23] NGI, ABIS, and CCD databases, and cites to appropriate privacy documentation, are discussed in this section below.

candidate as a match it is the responsibility of the HSI agent to update any information in IDENT/HART through existing methods after a candidate has been vetted and a lead validated.

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

CCD is the DoS repository for all visa and passport records.[24] It is used not only by the DoS as part of the visa adjudication process for biographic and biometric checks but also by DHS, the Department of Defense, and the Federal Bureau of Investigation (FBI). The CCD stores information about U.S. citizens and Lawful Permanent Residents (LPRs) who have filed for passports. It also contains information on foreign nationals who have filed immigrant and non-immigrant visa applications. CCD may also contain additional information stored submitted by federal agencies as a result of background checks on the individual. The CCD provides an FRS comparison against their database of visa records. An HSI agent may submit a probe photo to a CCD user to determine if an individual is in the database. CCD does not retain probe photos.

The candidate list will return all information associated with the individual contained within CCD. PII in a candidate return will only include matched images from visa and passport photos contained in CCD. HSI must then make a secondary request through the DoS Bureau of Diplomatic Security for additional information on an individual. This information could include biographic information, immigration information, contact information, financial information, medical information, legal information, educational information, biographic information on family and associates, derogatory information, and social media information (e.g., usernames listed on a visa application).

FBI Next Generation Identification System (NGI) Interstate Photo System

NGI is the FBI's primary identity management system. It contains biometric and criminal history records submitted to the FBI for criminal justice, national security, and civil purposes. The system has over 38 million criminal photos that are associated with a 10-print fingerprint scan.[25] NGI provides a facial recognition query capability to domestic law enforcement agencies to compare probe photos to its criminal photo gallery. Currently, before ICE can query NGI galleries via facial recognition, an HSI agent must open a cooperative case with the FBI, meaning that ICE and the FBI collaborate regarding an investigation that may implicate both agencies' statutory authorities. ICE would share the images with the FBI field office assisting with the case, and an agent from the FBI would submit the request for a query of NGI. All photos stored in the FBI NGI databases must be associated with a ten-print fingerprint. FBI will not maintain probe photos within NGI because probe photos are not associated with fingerprints. Probe photos may be

[24] *See* https://2009-2017.state.gov/documents/organization/242316.pdf.*See also* https://2001-2009.state.gov/documents/organization/109132.pdf.
[25] *See* https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

retained, however, in the FBI field office case file for investigative purposes.[26] NGI will always return multiple candidates from a query; anywhere from two to 50 photos may be returned. The ICE user submitting the probe photo can designate the number of candidates to be returned. The number of candidates may differ based on mission need, but HSI agents will be instructed to select a number that is considered best practices by law enforcement (e.g., 20 candidates) by default.

HSI also has the ability to request that the FBI field office use the FBI's Face Analysis, Comparison, and Evaluation (FACE) services unit.[27] This unit has trained facial examiners similar to those at OBIM who will manually review candidate lists generated by the algorithm to identify the most likely matches and ensure the quality of the candidate list.

Department of Defense (DoD) Automated Biometric Identity System (ABIS)[28]

ABIS is DoD's authoritative biometric system for matching, storing, and sharing biometrics in support of military operations. ABIS contains information on known or suspected terrorists, individuals deemed national security threats, DoD detainees, and individuals of interest to DoD. ABIS shares information with other federal agencies and DoD's foreign partners. ABIS has the functionality to conduct facial recognition queries. In the future, HSI may submit probe photos through IDENT/HART's connection with ABIS.

ABIS encounter information could contain data elements such as: ABIS encounter specific identifier, reason fingerprinted, date fingerprinted, associated derogatory information, the fingerprinting agency, associated biometrics (e.g., fingerprints), name, aliases, date of birth, place of birth, country of citizenship, and gender.

Commercial Vendors

Some commercial vendors maintain their own repository of images collected from either their own processes or searches of open source systems, obtained by "scraping" internet websites.[29] The images are unconstrained and may include multiple individuals. All collected images are available to the public. Vendors collect all images via simple searches. While HSI cannot directly control the means or methods of a vendor's data collection efforts, if HSI discovers that an FRS

[26] For more information on FBI case file retention and management *see* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/sentinel.

[27] *See* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

[28] For more information *see* Defense Biometric Services, 74 FR 48237 (Sep. 22, 2009), available at http://dpclo.defense.gov/privacy/SORNS/dod/A0025-2_SAIS_DoD.html, and Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007), available at http://dpclo.defense.gov/privacy/SORNs/dod/A0025-2c_SAIS_DoD.html. DFBA policy on biometrics are *available at* https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/852101E.pdf.

[29] Scraping is an automated process that retrieves websites, searches for and copies data that has been pre-designated by a user, then loads the copied data into a database for later use.

violates the privacy settings of an open source system, HSI will discontinue using that vendor's FRS.

Commercial vendors have also created facial recognition algorithms to query their proprietary databases. HSI has purchased licenses and/or paid for access to the FRSs of these vendors. HSI may upload an image to the vendor and require the vendor to delete the image immediately upon creation of a face template. A vendor may also provide a facial recognition query to compare one image in the vendor's database to other images in its database. In those instances, HSI will not upload any probe photos, but will select an image that was returned by conventional query method of the vendor's holdings (e.g., name search) and the vendor will use facial recognition technology to search for similar images.

The vendor's facial recognition technology will use available data to find images in its compiled dataset that match or are similar to the probe photo HSI uploaded or selected from the vendor's gallery. The vendor's technology will search all images in its gallery and all individuals that may be contained within an image in its gallery. If a vendor matches a candidate within an image containing multiple individuals, the vendor will isolate the facial image of the matched candidate within the candidate list. Therefore, HSI will only receive responses containing matched individuals. The returns are rank ordered so that images with the highest confidence scores are returned first. If an HSI agent is given the option by the vendor, he or she will opt for a limited number of returns (e.g., 20 candidates) rather than setting a confidence threshold.

The vendor will display any information it may have in its database associated with the image. Typically, this will include a link to the URL where the image was found so the investigator can go directly to the open source site. HSI would then capture and store relevant information obtained through the source URL. HSI agents will thoroughly check information derived from the open source site against government and public databases to either confirm or eliminate candidates prior to generating leads to send to the field for additional investigation.

Vendor facial recognition queries are treated as equivalent to open web searches via a search engine. HSI will not save the entirety of returned query results in ICE systems. Rather, HSI will only collect and document salient results as they pertain to the investigation.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[30] 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

[30] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[31]

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.[32] 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[33] and the Homeland Security Act of 2002 Section 222.[34] Given that HSI's use of facial recognition services spans multiple programs and activities, rather than comprises a singular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of Facial Recognition Services operations 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.

Notice of the existence, contents, and uses of FRSs by HSI is provided by the publication of this PIA and by the DHS/ICE-009 External Investigations System of Records Notice (SORN).[35] Since an FRS is a law enforcement tool that HSI uses to process sensitive information related to criminal investigations, it may not be feasible or advisable to provide notice to individuals at the time their image is collected or submitted as a probe photo. Some probe photos may be collected through other lawful means, such as by subpoenas and search warrants, and the record holder of those images are notified of the collection. If images are obtained from individuals through Federal Government-approved forms or other means, such as information collected pursuant to seizures of property, notices on the relevant forms generally state that the information may be shared with law enforcement agencies.

[31] 6 U.S.C. § 142(a)(2).

[32] *See* 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," *available at* www.dhs.gov/privacy.

[33] 44 U.S.C. § 3501 note.

[34] 6 U.S.C. § 142.

[35] DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010). This SORN is currently in the process of being updated.

Privacy Risk: There is a risk that an FRS will not provide adequate notice that its biometric collections may be used for facial recognition matching.

Mitigation: The risk is not mitigated. It is incumbent on the FRS to provide notice that images collected from individuals will be subject to facial recognition matching. Many FRSs use photographs collected for law enforcement purposes and background checks, such as mugshots and visa photos. These photos are collected directly from an individual and they are notified that the information can be used for law enforcement purposes. Some FRS galleries, such as DMV photographic galleries, collect photographs for purposes unrelated to law enforcement, but notify individuals generally that information collected could be used by law enforcement. However, HSI does not control the notice an FRS provides to individuals at the time of collection and cannot notify an individual when its agents use an FRS without informing a criminal suspect of an active investigation.

Privacy Risk: There is a risk that ICE uses unconstrained images and individuals will not have notice their image was used as a probe photo or that their information was obtained by HSI through an FRS.

Mitigation: This risk is being mitigated. Suspects in probe photos or identified via FRS data may not be advised they are being investigated. Notice to these individuals could inform them that they are the target of an actual or potential criminal investigation or reveal investigative interest on the part of DHS or another agency. Access to the records might also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, harm victims, or to avoid detection or apprehension.

All individuals present in the United States, however, have constitutional protections in criminal proceedings entitling them to discovery production.[36] The discovery obligations of federal criminal prosecutors are generally established by the Federal Rules of Criminal Procedure 16 and 26.2, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*,[37] and *Giglio v. United States*.[38] In immigration proceedings each party is responsible for producing evidence upon which it seeks to rely in the litigation. Therefore, if ICE seeks to use information derived from an FRS to sustain any charge or otherwise as evidence, it would produce that information.

[36] Discovery is the general process of a defendant obtaining information possessed by a prosecutor regarding the defendant's case.
[37] 373 U.S. 83 (1963).
[38] 405 U.S. 150 (1972).

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.

HSI will use an FRS when an individual cannot be identified or located via conventional investigative methods; therefore, the individual in question will generally not be able to individually participate in HSI's collection of probe photos or use of an FRS. In instances in which an individual participates in the collection of the photo (i.e., an individual suspected of identity fraud or whose phone contents are subpoenaed) there is no opportunity or right to decline to provide the images due to the law enforcement context in which probe photos are collected. These materials are potential evidence of criminal activity and are seized and used in accordance with criminal procedure.

FRSs that are maintained by federal, state, and local agencies generally collect images for their galleries directly from an individual. During the collection these agencies also collect biographic information from the individual 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 does 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) to which they applied.

Similar to notice, ICE does not control the access and correction procedures for FRSs. The ability for an individual to opt out of facial recognition queries or to access and amend information in a gallery is entirely dependent upon the FRS. All federal databases have access and amendment processes in place that are discussed in their relevant PIAs and SORNs.[39] State DMV databases similarly allow individuals to correct and update information online or in person at an office. An individual's ability to amend information in federal, state, or regional law enforcement information systems, however, is limited by law and policy due to the need to protect national security or law enforcement sensitive information.

For the same reasons, individual access to HSI holdings regarding probe photos, candidate returns, and/or vetting efforts are limited.[40] Individuals may submit requests for information and correction as permitted by the Privacy Act, and the requests will be reviewed and corrected on a case-by case basis. Individuals seeking to correct records, or seeking to contest their content, may submit a request in writing to the ICE Privacy and Records Office by mail:

[39] *See* footnotes 6-9.

[40] *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010), Final Rule for Privacy Act Exemptions, 74 FR 4508 (August 31, 2009).

U.S. Immigration and Customs Enforcement Privacy and Records Office
Attn: Privacy Branch 500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
(202) 732-3300
http://www.ice.gov/management-administration/privacy

Privacy Risk: There is a risk that individuals cannot access and amend inaccuracies in commercial vendor collections.

Mitigation: The risk is not mitigated. If a vendor FRS collects media from publicly available sources, any correction or update the individual makes to the information in the open source system might not be reflected in the vendor database. Moreover, vendors may not notify HSI when an update or correction occurs within its own proprietary database. HSI, however, will always research the source URL that originally contained information from a vendor FRS return to ensure that the information is as accurate, timely, and complete as possible prior to vetting a candidate and generating an investigative lead.

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.

ICE is authorized to collect information under Section 701 of the USA PATRIOT Act; 6 U.S.C. § 112; 8 U.S.C. §§ 1105, 1103(a)(4), 1357(a) and (b); and Executive Order 13388. Pursuant to the Homeland Security Act of 2002 (HSA), as amended, Pub. L. 107-296, 116 Stat. 2135 §§ 102, 102, 403, 441 (Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include laws contained in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this enforcement authority to the Director of ICE in DHS Delegation Order No. 7030.2, Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (Nov. 13, 2004), and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003). This authority has been delegated to HSI through ICE Delegation Order 73005.1, Immigration Enforcement Authority of the Director of the Office of Investigations (Mar. 5, 2007). Through these statutes and orders, HSI has broad legal authority to enforce an array of federal statutes including responsibility for enforcing U.S. civil immigration authorities, customs authorities, and federal criminal authorities. HSI investigates all types of cross-border criminal activity, including financial crimes, money laundering, and bulk cash smuggling; commercial fraud and intellectual property theft; cybercrimes; human rights violations; human smuggling and trafficking; immigration, document, and benefit fraud; narcotics and weapons smuggling/trafficking; transnational gang activity; export enforcement; and international art and antiquity theft.

HSI will only submit probe photos to be used in furtherance of ongoing criminal investigations. Under this PIA, ICE's Enforcement and Removal Operations (ERO) will not use and HSI will not support ERO in using FRSs solely in furtherance of civil immigration enforcement. HSI will only submit probe photos that are linked to ongoing criminal investigations for crimes HSI has the statutory authority to enforce. ICE stores all probe photos and results of an FRS queries in an ICE system of records and maintains them in accordance with the Privacy Act of 1974.[41] HSI's collection, use, and maintenance of this information is covered under the DHS/ICE-009 External Investigations SORN.[42]

Privacy Risk: HSI may use an FRS for purposes beyond what is described in this PIA.

Mitigation: This risk is being mitigated through training and oversight. HSI, DHS S&T, and ICE Privacy will create a training and Rules of Behavior (ROBs) for HSI agents that details the restraints and safeguards outlined in this PIA. Federal and state FRSs also require that probe photo submissions be associated with an ongoing law enforcement activity by requiring the agent to state the violation he or she is investigating. Some commercial vendors also log FRS queries/returns and make those logs available upon request. ICE Privacy will only approve the use of a commercial vendor that provides auditing capabilities. HSI supervisors will regularly audit agent case files to ensure that the source of probe photos, the necessity and relevance of an FRS, the use of an FRS, and the name of the FRS are noted as an ROI in ICM. ROIs must be approved by a supervisor before they are considered final and available for viewing by other ICM users, ensuring that HSI supervisors will oversee agent use of FRSs. Candidate returns and leads generated will also be noted as ROIs within ICM. As such, accountability regarding the collection, sharing, and receiving of information in connection with an FRS will be similarly overseen and audited by HSI supervisors. Finally, ICM entries are routinely audited by the ICE Office of Professional Responsibility (OPR) to ensure proper use of the system and proper handling of evidence in investigations. Agents found to be mishandling evidence, including probe photos, face disciplinary action by ICE.

[41] 5 U.S.C. § 552a.

[42] *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010). This SORN is currently in the process of being updated.

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).

HSI will extend its existing policies and oversight regarding evidence gathering and handling to its collection of probe photos to ensure only the minimum amount of data required for an investigation is collected. HSI agents only collect information in furtherance of their statutory law enforcement authorities for the purposes of furthering an ongoing investigation. Probe photos will always be obtained either via open source systems, government databases, or proper law enforcement requests and activities.

HSI will not collect probe photos from individuals actively exercising rights protected by the First Amendment to the United States Constitution (e.g., at religious services or political protests). During the FRS submission process, HSI will only create probe photos from individuals suspected of participating in or being victimized by a crime under its legal authority. HSI will only submit still images of a single face as a probe photo to an FRS. ICE Privacy, DHS S&T, and HSI are developing a training for HSI agents, in consultation with ICE attorneys and the DHS Office for Civil Rights and Civil Liberties, that will cover these restrictions on collections. HSI supervisors will also be trained to review FRS requests and ROIs by their agents to ensure adherence with these practices.

Probe photos and candidate returns will be maintained within the relevant case file. Case files are retained for 20 years after the case is closed in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B).[43] ROIs within ICM connected to the case will similarly be deleted 20 years after case closure. An ICE-wide updated schedule for investigative records is being developed and will be submitted to the National Archives and Records Administration (NARA) for approval.

Privacy Risk: An FRS may return excessive amounts of candidates, leading to an overcollection of individual information irrelevant to the ongoing criminal case.

Mitigation: The risk is being mitigated. Some FRS agencies and vendors allow a law enforcement agency the option of setting the maximum number of candidates to be returned from a query. If the FRS has the functionality, then the HSI agent will select as a default a number that is considered best practice by law enforcement (e.g., 20 candidates) returned per query. Returns should be large enough to reduce the impact of false positive matches from an FRS because it

[43] Records retention is made in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.

increases the likelihood the correct individual is among the candidates. HSI vets multiple individuals to create a lead and HSI cannot rely on the match alone as verification that the candidate matches the probe photo.

If an FRS returns similarity scores with a candidate list HSI will use those scores to triage its vetting process. Candidates with low similarity scores may not be vetted if HSI can confirm an identity in a return. Only successfully vetted candidates will be entered into ICM as an ROI. Information regarding candidates returned by an FRS that were unsuccessfully vetted by HSI will only be maintained in the external case file at the local HSI office where the investigation is occurring per the Federal Rules of Evidence. That information cannot be searched by personal identifier and will not be used by HSI for any other purpose.

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: The risk is mitigated. The 20-year retention period for ICM and other case file records is consistent with the retention schedules for other investigative records within DHS. By ensuring that information pertaining to individuals who are encountered repeatedly over a span of time can be linked, this retention period supports HSI's effective enforcement of U.S. civil immigration authorities, customs authorities, and federal criminal authorities. Closed cases can contain information that may be relevant to a new or existing case and need to be readily searchable and accessible for at least a period of time. The addition of probe photos and candidate returns to a case file will not affect the existing retention processes in ICE systems. Probe photos and candidate returns will be destroyed when the case file is destroyed.

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 use and sharing of probe photos by HSI will only be for purposes compatible with the original purpose for collection, which is to conduct criminal law enforcement investigations and other immigration enforcement activities, to uphold and enforce the law, and to ensure public safety. HSI limits the use of FRSs to ongoing investigations when conventional investigative means have been unsuccessful in identifying or locating a subject. HSI personnel will be trained so that they do not use an FRS to surveil the public. HSI agents do not have the capability and will not attempt to procure any device that allows an FRS to analyze live video, streaming media, or any other surveillance device in real-time.

All external sharing falls within the scope of applicable law, including the published routine uses in the DHS/ICE-009 External Investigations SORN, in particular routine use J, as any

FRS submission would be to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation. HSI will ensure that probe photo use and disclosure is within the proper performance of the official duties of the agent making the disclosure.

Privacy Risk: HSI may submit images that are not directly relevant to an ongoing criminal case.

Mitigation: This risk is being mitigated. HSI personnel will receive training that details the appropriate uses of an FRS, including the requirement that all submitted images be relevant to an ongoing investigation. HSI agents will note the source of collection for probe photos in the investigative case file and as part of an ROI in ICM. HSI supervisors will review ROIs to ensure that probe photos were collected from an appropriate source for an appropriate purpose and the FRS used was necessary and relevant to further the investigation. ICM entries are routinely audited by the ICE Office of Professional Responsibility (OPR) to ensure proper use of the system and proper handling of evidence in investigations. Agents that are found to be mishandling evidence, including probe photos, face disciplinary action by ICE. Probe photos and resulting information that were inappropriately submitted or collected are deleted upon discovery of inappropriate conduct.

Privacy Risk: HSI may investigate candidates returned from an FRS who have not been properly vetted or are not linked to the probe photo.

Mitigation: This risk is being mitigated through auditing and oversight of HSI investigative activities. HSI supervisors routinely review their agents' case files and inspect generated leads as part of their review. Any lead received by an HSI program or office is routinely reviewed by an HSI Supervisor prior to assigning the lead to an agent to follow up. Ultimately, any investigative activity by an HSI agent must be entered into ICM as an ROI or a subject record. ROIs must be approved by a supervisor before they are considered final and available for viewing by other ICM users. In contrast, Subject Records created by ICM users are immediately viewable to other ICE users because of the need to deconflict them (and because of officer safety concerns), but they are flagged to indicate they are pending until a supervisor reviews and approves them. Copies of ICM records are not placed in the HSI Data Warehouse[44] until they are approved. HSI supervisors will ensure that HSI investigative activity is only conducted through appropriate means and will delete any records obtained improperly by an agent. Further, the agent may be disciplined for improper use of the FRS returns and referred to ICE OPR.

[44] The HSI Data Warehouse is a data storage environment that serves as a repository for ICM system data. It receives a direct feed once every 24 hours containing a refresh of ICM data, including new records and edits to previously existing records. For more information on HSI Data Warehouse *see* DHS/ICE/PIA-045 ICM.

Privacy Risk: An FRS may use images submitted by HSI for purposes other than its original collection.

Mitigation: The risk is being mitigated. HSI will review FRS terms of service and policies to ensure that all FRSs it uses, including commercial vendors, will not re-disseminate probe photos and will delete probe photos immediately after a face template is created. In cases of exigent circumstance where an FRS cannot be vetted prior to submission of a probe photo, HSI will engage with the FRS directly after the submission to ensure the submitted photo was deleted. The government agencies with which HSI engages for FRS have authorities and missions consistent and compatible with the authorities and mission of DHS, ICE, and HSI, thereby reducing the likelihood any agency uses a probe photo for purposes outside of law enforcement or public safety. Moreover, HSI will only send the probe photo of the subject without contextual information. The probe photo would be of limited value to the FRS without any associated information.

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 Recognition algorithms have become exponentially more accurate over the past decade. However, due to the novelty of the technology and potential for error, HSI only uses FRS returns as the first step in an investigative process. Results of FRS processes can vary on a case by case basis. This is because the accuracy of an algorithm used by FRSs varies among agencies and vendors and similarity thresholds are not standard across FRSs.

Moreover, the quality of submission by HSI agents can affect the accuracy and integrity of the FRS candidate returns. For example, the lighting, sharpness, and resolution of the image will all affect the accuracy of the FRS. Further, a subject’s angle to the camera, expression, or occluding features (e.g., facial hair, sunglasses) will affect each FRS algorithm differently. DHS S&T will be working with HSI and ICE Privacy on proper collection and isolation techniques (e.g., zooming, cropping) to reduce variations between a probe photo and an FRS’s image gallery.

As the variation in accuracy and biases in FRSs used by HSI cannot be controlled by ICE, HSI ensures that each candidate return from an FRS is given proper weight in the investigative process. HSI agents are continually trained to know that candidate returns are leads only, and not a positive identification. Candidate returns are not used as an indicator of unlawful activity or used to establish probable cause. HSI agents only use a vetted candidate match as the first step in the investigative process and are required to compile validating evidence of the match.

Privacy Risk: There is a risk HSI will submit low quality images or probe photos that would otherwise increase the likelihood of false matches from an FRS.

Mitigation: The risk is being mitigated. Most FRSs exercise quality control of images accepted into their systems. As the biometric service provider, the FRS can reject a probe photo that is of too low a quality to produce a candidate list to the designated confidence threshold. Some FRSs offer users specialized training that details proper collection techniques, selection criteria, and cropping techniques for probe photos for use of their gallery. As part of their terms of service, some of these FRSs require a requestor to certify that he or she has taken the training prior to submitting a probe photo or receiving access to upload probe photos. Additionally, ICE Privacy will be working with HSI and relevant stakeholders to develop a training HSI agents will take to maximize image quality prior to FRS submission.

Privacy Risk: There is a risk an FRS will misidentify individuals in the facial recognition process. This risk is increased because ICE may not have control over the accuracy standards or thresholds set by third party FRS technologies.

Mitigation: The risk is being mitigated. FRS technologies return lists of candidates and do not make positive identifications of any individual. Candidate lists reduce the impact of potential false positive matches by an FRS. This is because lists remove the certainty of positive identification on biometrics alone and requires HSI to vet multiple individuals to create a lead as different individuals may share different biometric traits. Therefore, HSI cannot rely on FRS results alone as verification that a candidate return matches the probe photo. In cases in which HSI requests review by a trained facial examiner, the algorithm will still return a list of multiple candidates, and a trained biometric examiner will act as a further check for accuracy against an FRS return. A return from a facial examiner will result in a smaller candidate list being returned from the FRS but will be accompanied by the same disclaimers stating that candidates must be vetted and that information should be used for lead purposes only. HSI will not use lists returned by an FRS for any lead or law enforcement action without additional research and analysis, even if a trained facial examiner from an FRS has narrowed the list to one candidate. HSI agents will cross check FRS returns against government databases and open source information, such as news articles or public records, to vet potential matches. Finally, possible matches are considered investigative leads until HSI agents gather additional evidence that validates the potential match.

Privacy Risk: There is a risk that HSI will use biographic or derogatory information received from an FRS that is inaccurate.

Mitigation: This risk is being mitigated. The original collection of the data by federal and state/local FRSs will be from the individual directly. Data returned by intelligence fusion centers are gathered for law enforcement and/or national security purposes. Law enforcement and national security personnel are trained to review all information they collect for accuracy, as errors may detrimentally affect prosecutions and investigations. This increases the likelihood that the information within a fusion center has been previously vetted for accuracy. Commercial vendor FRS returns link directly to the source material from which the data is collected, allowing HSI agents to collect data directly from the source. Additionally, HSI will conduct its own research and investigation to determine if the information returned by an FRS is accurate before taking any enforcement action.

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.

The HSI office making an FRS request is responsible for the security of PII transmitted and received. HSI agents accessing an FRS follow ICE standard technical and organizational safeguards that protect against unauthorized disclosure, alteration, access, or use of PII and SPII. Each FRS will have its own procedures for submitting and receiving information. OSDM or an HSI supervisor must approve any FRS prior to HSI submitting probe photos. In that approval, OSDM must ensure that the FRS takes reasonable measures so only authorized individuals have access to the PII exchanged. OSDM will do this prior to a probe photo submission, or in the cases of exigent circumstances, as soon as possible thereafter. The agent and the supervisor will also ensure that transmission and receipt of information while using an FRS are appropriately encrypted in accordance with DHS standard operating procedures in the safeguarding of sensitive PII[45] and ICE standards on the handling of law enforcement sensitive information. OSDM will also check that the FRS's terms of service and data security polices state that it does not retain any probe photos sent by HSI or share probe photos with other parties.

Information retained by HSI, including probe photos and candidate returns, are secured through ICM. The ICM system actively prevents access to information for which a user lacks authorization, as defined by the users' need to know and job responsibilities. The user who created a case or record in ICM may limit the access by others to that information, except for the originator's supervisor. HSI agents are required to complete ICM-specific, role-based training before being granted an ICM account.

Privacy Risk: There is a risk that an FRS will mishandle HSI data, leading to a data breach or privacy incident.

Mitigation: This risk is being mitigated. HSI's submission to an FRS will only contain the minimum amount of information necessary for the FRS to run a biometric query. Usually this only involves the case agent name, the probe photo, and the statutory violation being investigated. If a breach occurs, the information lost by the FRS will be minimal and without context. OSDM will also ensure that the FRS's policies require it to delete the probe photo after its algorithm

[45] For more information *see* DHS Handbook for Safeguarding Sensitive PII *available at* www.dhs.gov/privacy.

creates a face template or finishes a search. All that would remain in an FRS database would be the case agent name and a log of the request itself.

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.

HSI's use of FRSs is an extension of its existing investigative processes. Therefore, the auditing and oversight of FRS use is in keeping with the handling of any sensitive evidence maintained in the HSI Investigatory Case Management system (ICM). The HSI supervisor will regularly audit investigative case files to ensure that the use of an FRS and the name of the FRS are documented as an ROI in ICM. Candidate returns and leads generated will also be recorded as ROIs within ICM. As such, accountability checks regarding the collection, sharing, and receiving of information in connection with an FRS is dependent on HSI agents following HSI standard procedures and requirements for logging information in the ICM case management system. Additional specifics regarding ICM's auditing and accountability procedures can be found in the ICM PIA.[46]

The access controls, auditing, and supervisory review of ICM case files ensure information is used in accordance with the stated practices in this PIA. The HSI case agent receives a query notification whenever another ICM user has viewed a document of theirs in the system. Using this functionality, users can "police" their records, including ROIs and Subject Records, by having notice and the ability to inquire as to why another user has conducted a particular query. Query notifications bring transparency to the system that discourages unauthorized browsing for information. If an HSI case agent suspects or has reason to believe ICM records have been misused in any fashion, the agent must report the suspected misconduct to OPR for further investigation.

Finally, ICM maintains detailed sets of auditing requirements that are tracked and saved in audit logs that can be later viewed by OPR if allegations of misuse are made against an ICM user. ICM keeps copies of audit and log file data in a separate data repository where they are retained for seven years to ensure ICE will be able to track and investigate misconduct and misuse of the system. OPR users who query ICM and the HSI Data Warehouse also have their activity tracked in the audit logs. However, their queries and viewing of ICM case records do not trigger notifications to the case agent in order to preserve the integrity and confidentiality of ongoing OPR investigations.

[46] DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), available at https://www.dhs.gov/privacy-impact-assessments.

Conclusion

Facial Recognition Technology is a rapidly developing capability that is already in use by law enforcement agencies nationally. ICE HSI's mandate to safeguard the nation and enforce immigration laws are aided exponentially through the use of third-party services that use facial recognition technology. While the technology itself does have far reaching privacy implications, HSI has established processes and procedures to mitigate the impact of an FRS on individuals. Through proper collection techniques, candidate vetting, and supervisor oversight, HSI endeavors to use FRSs in as much of a privacy sensitive manner as possible.

Responsible Officials

Jordan Holz
Privacy Officer
U.S. Immigration & Customs Enforcement
Department of Homeland Security

Approval Signature

[Original, signed copy on file with the DHS Privacy Office]

____
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security