Homeland Security Investigations

U.S. Department of Homeland Security
500 12th Street, S.W.
Washington, DC 20536

U.S. Immigration and Customs Enforcement

MEMORANDUM FOR: All HSI Personnel

FROM: Matthew C. Allen
Acting Executive Associate Director

MATTHEW C ALLEN Digitally signed by MATTHEW C ALLEN
Date: 2021.01.15 14:01:36 -05'00'

SUBJECT: Use of and Access to Third-Party Facial Recognition Services

1. Purpose and Applicability

As part of its criminal and administrative law enforcement missions, U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) relies on a variety of law enforcement tools and techniques to ensure public safety and national security. Facial recognition technology and services provide an important tool to support HSI mission activities. To maximize the use of this tool consistent with privacy, civil rights and civil liberties requirements, this memorandum provides HSI personnel with guidance on the acceptable use of Facial Recognition Services within the scope of their official duties.

This memorandum only pertains to the use of third-party facial recognition technologies and does not apply to any internal system or technology HSI may acquire and/or develop at a future date. This memorandum also 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. Moreover, this memorandum only covers the actions of HSI personnel fulfilling their statutorily authorized duties. It is not meant to provide guidance or authorization for other offices within ICE to access or use facial recognition technologies or services.

2. Definitions

Facial Recognition Technology: A system that uses algorithmic analysis to compare facial features between images to determine the likelihood that those images depict the same individual. For purposes of this memorandum, facial recognition technology is used to verify that an individual in a submitted image is the same individual depicted in a selected image within a database (1:1 match); compare the likeness between two submitted images (2-photo submission); or identify an unknown individual by analyzing a gallery of images in a database to find an image similar to a submitted image (1:many match).

Facial Recognition Services (FRS): A government agency or commercial vendor who manages its own image database(s) and chooses its own facial recognition technology. These agencies and vendors accept facial image submissions from third parties, including HSI, to run comparative queries of their own image galleries using their own facial recognition algorithm.

Probe Photo: Isolated facial images that are lawfully obtained pursuant to an authorized criminal investigation and submitted for facial recognition matching.

Candidate List: An algorithmically generated list of images from a database where one of the images in the database may be the same individual that appears in the submitted photograph. Usually, the list is ranked in order by the likelihood that the images contained within the database match the probe photo submission. A recipient must review the candidate list to determine whether a potential match exists. No candidate list return will be relied upon for positive identification.

Exigent Circumstances: Circumstances that will cause a reasonable person to believe that immediate action is necessary to prevent physical harm to the officers or to other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.

3. HSI's Use of Facial Recognition Services Data and/or Technology

HSI personnel may use an FRS for purposes of an HSI investigation and/or joint investigation with another law enforcement agency for authorized law enforcement purposes relating to HSI's statutory authorities and law enforcement mission. HSI personnel may only share information obtained from the use of an FRS with other parties or entities as authorized by statute, regulations, and/or existing information sharing agreements.

HSI personnel may use an FRS in four ways:

(b) (7)(E)

4. Requirements for Use of Facial Recognition Services

A. General Requirements

1. HSI will use an FRS only for authorized law enforcement purposes. Authorized law enforcement purposes require that HSI's use must be either:
    - Relevant and necessary to an ongoing investigation relating to HSI's statutory authorities; or
    - Part of an established HSI program or task force whose use of facial recognition is assessed for its impacts on privacy, civil rights and civil liberties.
2. Prior to using an FRS, HSI will use reasonable efforts to identify, locate, or verify an individual through traditional investigative means and methods.
3. Prior to using an FRS, HSI personnel will certify through the Performance and Learning Management System (PALMS) that they:

- Have completed an HSI and Office of Information Governance and Privacy (IGP) approved training course on Facial Recognition Technology, titled ICE Use of Facial Recognition Services, found on PALMS;
- Will use best practices, as outlined in the training, when collecting probe photos, submitting photos to an FRS, and using candidate lists returned from an FRS; and
- Will abide by the privacy, civil rights and civil liberties safeguards set forth in the training, the Privacy Impact Assessment published at

(b) (7)(E)

B. Collection of Probe Photos.

1. HSI personnel may collect probe photos of a potential suspect or victim of a crime or administrative violation under a HSI investigation.
2. HSI personnel may only collect probe photos of witnesses to crimes if supervisory approval is obtained and other reasonable methods to further an investigation have been exhausted.
3. HSI will not collect probe photos of individuals based solely on:
    - Religious, political, or social views or activities;
    - Participation in a noncriminal organization or event protected by the First Amendment; or
    - Race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, nationality, or any individual characteristic protected by law.
4. HSI will not use an FRS to surveil the general public. An FRS will not be used real-time in conjunction with surveillance or live streaming media. The Assistant Director for IGP and HSI Assistant Director Level leadership, in consultation with the Office of the Principal Legal Advisor, will separately assess future legal or technological FRS developments for additional guidance.

C. Submission to an FRS

1. HSI personnel will only submit probe photos to an FRS that has been reviewed and approved by the HSI Operational Systems Development and Management unit (OSDM) of the Operational Technology and Cyber Division, except in cases of exigent circumstances.[1]
2. The OSDM approved FRS list is found at

(b) (7)(E)

3. In the case of exigent circumstances, an HSI supervisor must approve the use of any FRS that has not been reviewed and approved by OSDM. The supervisor must provide his or her approval prior to use of the FRS where possible, or as soon as practicable thereafter.
    - Any FRS used in cases of exigent circumstance will be submitted to OSDM for subsequent review.

[1] The OSDM review and approval process is documented in the ICE Use of Facial Recognition Services PIA.

- HSI personnel are prohibited from using an FRS that has been reviewed by OSDM and not approved for use, even in exigent circumstances.

4. HSI personnel will use an FRS in accordance with the terms and conditions of that FRS.

D. Receipt of Information from an FRS

1. HSI personnel, unless specifically trained and authorized, will not act as biometric facial examiners.
2. No Candidate lists will be considered a positive identification. HSI Personnel will compare information contained in candidate lists with other information obtained using traditional means and methods to determine whether potential matches may result in a lead for an investigation.
3. All potential matches will only be considered investigative leads by HSI. HSI will not take enforcement action based solely on data collected from FRS databases. FRS data will be supplemented with other investigative information before taking enforcement action.

E. Auditing and Accountability.

1. Any submission to an FRS will be noted in an office or program log or system logging mechanism detailing the FRS used, the personnel that submitted the probe photo, and the case and/or violation associated with the submission.[2]
2. All results of an FRS used in a case will be noted in a report of investigation in the relevant case file and in the HSI **(b) (7)(E)**
3. OSDM has established the **(b) (7)(E)** and **(b) (7)(E)** Program Code: **(b) (7)(E)** **(b) (7)(E)** Use of the FRS Program Code is mandatory.
4. HSI front-line supervisors will review logs, case files, and **(b) (7)(E)** entries routinely to ensure compliance with this guidance. Non-compliance, including inappropriate access and use, may be referred to the ICE Office of Professional Responsibility (OPR), when appropriate.
5. ICE OPR will conduct regular audits to ensure compliance with this policy.

5. No Private Right of Action

This memorandum may be modified, rescinded, or superseded at any time without notice. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.

Likewise, no limitations are placed by this guidance on the other lawful enforcement or litigative prerogatives of ICE.

Direct questions about this guidance to the IGP Privacy Uni **(b) (7)(E)** *@ice.dhs.gov).*

[2] Log format and the manner of log storage and accessibility will be submitted to IGP for approval.