Privacy Impact Assessment
for the

War Crimes Hunter

DHS/ICE/PIA-056

May 28, 2020

Contact Point
Alysa Erichs
Acting Executive Associate Director,
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

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

Abstract

War Crimes Hunter (WCH) is a program, run by the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Human Rights Violators and War Crimes Unit (HRVWCU), that collects and shares information about alleged human rights violators. HRVWCU is dedicated to identifying, locating, investigating, prosecuting, and removing human rights violators from the United States, as well as preventing their initial entry into the country. WCH collects digital media depicting individuals engaged in war crimes and human rights violations, isolates the facial images of the suspected perpetrators, and shares those images with the biometric databases of relevant Federal partners. These partners search their databases for potential matches based on facial recognition alone and return lists of candidates that HRVWCU can use to produce investigative leads. ICE is conducting this Privacy Impact Assessment (PIA) because WCH collects and disseminates personally identifiable information (PII) of individuals who are located overseas and engaging in human rights violations.

Overview

ICE established HRVWCU in 2003 to strengthen the agency's efforts to identify and investigate individuals involved in war crimes and human rights abuses around the world.[1] The unit draws on the skills and experience of special agents, historians, intelligence analysts, and attorneys; and works with interagency partners to: (1) prevent the entry of human rights violators into the United States, and (2) arrest, prosecute, and/or remove human rights violators already in the United States. Since 2003, HRVWCU has prevented over 300 entries of human rights violators and war criminals into the United States. More than 450 individuals have been arrested for human rights-related violations of the law under various criminal and/or immigration statutes, and over 1,000 known or suspected human rights violators have been removed from the United States. The unit currently oversees more than 180 active investigations and is pursuing hundreds of leads involving suspected human rights violators throughout the world.

HRVWCU researches both on-going and past atrocities. Through WCH, HRVWCU will collect digital images of individuals engaged in human rights violations occurring overseas. These images will be collected from publicly available, open-source web-based media sites identified as relevant and credible by HRVWCU. From this collection, WCH users will isolate relevant facial images of perpetrators to create a database of suspected human rights violators. HRVWCU will share these images with Federal biometric and biographic databases that partner with HRVWCU.[2]

[1] The human rights abuses and war crimes about which WCH will collect images include torture, genocide, recruitment and use of child soldiers, extrajudicial killing, and particularly severe violations of religious freedom. *See* Section 1.0 of this PIA for the specific statutory citations.
[2] These agencies are referred to as "partners," "partner agencies," or "WCH partner agencies" throughout the PIA.

The partner will then compare images against their existing facial biometric data holdings using facial matching methodologies.[3]

WCH will be used as an investigative tool to develop leads that will require additional investigation by HSI personnel. Leads are considered the first step in an investigative process and are not proof of criminality or a positive identification. Leads cannot be solely used to deny immigration benefits, or establish probable cause to conduct a search, arrest, or similar law enforcement action.

Data Collection

WCH will collect media from publicly available websites identified by HRVWCU as containing images of human rights violations or violators. HRVWCU will focus on websites whose content and subject matter are focused internationally. These websites and the media that WCH collects are available to any member of the public and are maintained by a variety of entities, including perpetrators, journalists, international organizations, and human rights organizations. WCH users will use all evidence at their disposal, such as witness statements, human rights reports, other HRVWCU leads, and other documentary evidence, to determine the veracity and authenticity of the site and its contents prior to collecting media from the site. The site is then submitted to a HRVWCU supervisor for approval to collect.

Once a HRVWCU supervisor has verified that a website has relevant and credible evidence of human rights violations, it will be designated for automated on-going collection by the WCH tool. The WCH tool will routinely capture and preserve media presented on designated sites automatically and load the media into the WCH repository for review. The WCH tool does not modify the image in any way. All collection by the WCH tool will be passive. The technology will not violate or circumvent paywalls or privacy settings and protections placed on the media by a website. The WCH tool does not search individuals' social media posts, but third-party websites from which WCH collects data may contain posts that were derived from individual social media accounts. For example, if a news outlet posted evidence of a war crime it collected from an individual's social media account, the WCH tool could theoretically collect that media from the news outlet's website. The WCH tool does not friend or follow social media accounts, will not post content on social media websites, and will not induce any website to collect information from other individuals or accounts. All collections are manually reviewed by a WCH user for credibility and relevance to the WCH mission. If media collected by WCH is deemed irrelevant, then HRVWCU deletes this information and it will not be stored or retained in the WCH repository. If at any point a site is determined to no longer be relevant to HRVWCU operations, the collection will be discontinued. Similarly, if HRVWCU becomes aware that a site may no longer present

[3] Facial matching methodologies include automated facial recognition and/or manual face examination by trained examiners. The processes and technologies of each partner's database is detailed in their own privacy compliance documentation, cited in the appendices of this PIA.

credible information, then automated on-going collections will be discontinued.

Some of the captured media might contain images of non-participants or witnesses to human rights violations. To address this issue, HRVWCU will incorporate a technology to blur the faces of non-participants in the original media that was collected. WCH will store collected media in a secure repository for possible future use as leads, or in administrative or criminal proceedings, or for HRVWCU's efforts to prevent perpetrators from entering the United States.

WCH will use image analysis software to detect faces in the stored media to aid WCH user review. WCH users will review the WCH media and isolate facial images of suspected perpetrators. Additionally, a WCH user will confirm all isolated images are of suspected human rights violators prior to sharing with partners, in order to mitigate the potential of sharing bystander images. Both the blurred media and the isolated images will reside in the WCH repository. During this review process, the WCH user will select isolated images that are best suited for facial recognition processes. The WCH user will ensure he or she isolates a facial image that has the highest image quality possible, contains the fewest obscurations of the perpetrator's face, and is most similar to a "constrained image,"[4] such as a mugshot or passport photograph. This is because WCH endeavors to isolate images as similar as possible to the galleries of images held by its partners. WCH users will continually refine their image gathering techniques through ongoing discussions with partner agencies.

The WCH user will catalog the collected media by relevant statutory inadmissibility charge(s) (e.g., genocide, extrajudicial killing, use and recruitment of child soldiers, torture). The WCH user will then format a perpetrator's facial image for sharing with DHS components and Federal agencies that have biometric database(s) and have executed an information sharing agreement with HRVWCU.[5] All HRVWCU personnel responsible for analyzing and sharing facial images with partners will be provided the appropriate privacy training prior to accessing WCH and will be supervised by a HRVWCU supervisor.

Sharing with WCH Partner Databases

HRVWCU intends to share isolated facial images of alleged perpetrators with partner agencies who will subsequently run queries against their biometric holdings. WCH partner agency biometric databases are listed in the appendix(s) of this PIA, and new appendices will be added as new partners join the program. WCH will format images in accordance with the National Institute

[4] A "constrained image" refers to an image that is standardized in format, lighting, distance to subject, and expressions.

[5] War Crimes Hunter will only share unmatched images with Federal partner agencies for purposes of biometric matching. HRVWCU, however, shares other, law enforcement information with state, local, tribal, foreign, and intergovernmental agencies to fulfill its law enforcement missions.

of Standards and Technology (NIST) standard transmission format prior to submission.[6] The NIST standard dictates file content, type, and units of measurement, as well as encoding instructions, required for electronic exchange of biometrics. WCH will transmit to partners the facial image of the violator, numeric identifiers assigned by WCH that correspond to the subject, and alphanumeric identifiers linking the image to the source media from which the face image was collected.

Each partner agency will establish ongoing information sharing practices with HRVWCU. The details of each connection will be documented in the respective appendices of this PIA. Prior to receiving WCH data, a partner must confirm it has adequate privacy protections. HRVWCU will leverage existing or execute new Information Sharing and Access Agreements (ISAAs) to share images with non-DHS Federal agencies. These ISAAs are reviewed by the ICE Privacy Division, ICE attorneys, the DHS Privacy Office and/or other DHS Oversight bodies[7] to verify that information safeguards and privacy protections are in place. The agreement may, as a matter of DHS policy, stipulate additional access, correction, or redress procedures for DHS data shared with an external partner. Similarly, HRVWCU will work with the aforementioned offices and divisions to ensure privacy protections are in place for biometric databases owned by other DHS components. During this process HRVWCU will enter into an Interconnection Agreement with that component. The partner agency's system(s) would then store and match the face images against its own biometric repositories. The transfer, retention, and uses of WCH data by partners is outlined in the appendix(s) of this PIA. ICE will add appendices to this PIA as partner agencies join the program.

Facial Recognition Process

Upon receipt of a facial image search request from WCH, agency partners will initiate a Facial 1 to Many (candidates) search of their existing facial biometric data holdings according to their internal agency procedures. Each agency partner's image analysis technology is covered in depth in its privacy compliance documentation, cited in the appendices to this PIA. The agency partner's search will not result in a single identity match, but rather in a ranked candidate list of

[6] ANSI/NIST-ITL 1-2011, 2015 Update (or most recent), *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information* (https://www.nist.gov/programs-projects/ansinist-itl-standard).

[7] The DHS Data Access Request Council (DARC) is the coordinated oversight and compliance mechanism that reviews bulk transfers of data in support of DHS's national or homeland security missions. The DARC ensures bulk sharing initiatives or activities comply with applicable law and adequately protect the privacy, civil rights, and civil liberties of the individuals whose information is shared. The DARC includes representatives from the DHS Privacy Office, Office for Civil Rights and Civil Liberties, and the Office of the General Counsel, collectively known as "DHS Oversight Offices." The DARC also includes representatives from DHS Components, including Component privacy officials and mission representatives. Part of the DARC's review of sharing agreements includes assessing whether appropriate access, correction, and redress procedures exist, and these procedures are documented in the ISAA.

potential matches based on similarity scores.[8] A similarity score is what the technology determines to be the likelihood that two images contain the same individual. The partner will then have potential matches reviewed by trained biometric face examiners. The examiners will cull the candidate list using analysis of unique facial features called "morphological analysis."[9] Face examination and reporting processes are based on best practices established by the Facial Identification Scientific Working Group (FISWG),[10] which operates under the NIST-run Organization of Scientific Area Committees (OSAC) for Forensic Science. The examiners will parse the list of candidates to only those assessed to be potential matches. The partner will provide WCH a narrowed candidate list which may contain the corresponding candidate's image(s), associated unique identifiers (e.g., Fingerprint ID number),[11] as well as a confidence level score, which is the examiner's explanation of the likelihood of matches between analyzed images. As needed, WCH users can request access to additional information pertaining to a particular candidate's encounter and derogatory information that may be contained within the Partner's system.

Lead Generation and Referrals to the Field

Any data collected by WCH will be vetted by HRVWCU to ensure its accuracy. HRVWCU personnel will not act as adjudicators or examiners for image matching, as HRVWCU does not have the technical capability. Partner confidence/similarity scores, if provided, will only be used as a triage tool for HRVWCU research and vetting, not as an indicator of any criminal activity. HRVWCU will compare information received from partners to other information available to HSI from various sources to vet the potential match. In some cases, additional biographic, encounter, and derogatory information about a potential match will be obtained directly from the partner to assist in the vetting process. When the vetting process is complete, HRVWCU will enter relevant information into the ICE Investigative Case Management system (ICM)[12] for further investigation by a relevant HSI field office. This is known as "lead generation." All leads undergo a final review by an agent and analyst from HRVWCU, as well as an ICE attorney. This review is to confirm the validity and accuracy of the information as well as its legal sufficiency before submitting to the field for further investigation by HSI agents. HRVWCU will note the lead in ICM. The source of the information and the fact that the lead was derived from facial recognition matching will be noted in a report made in ICM. Candidate lists will be maintained in an external investigative case

[8] Candidate list lengths and matching thresholds are partner dependent and is described in the appendices of this PIA.
[9] *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.
[10] For more information *see* https://fiswg.org/about_swgs.html.
[11] Information returned by each partner is detailed in the Appendices of this PIA.
[12] *See* DHS/ICE/PIA-044 Investigative Case Management System (ICM) *available at* www.dhs.gov/privacy. Should ICE enter this information in other IT systems, ICE will update the relevant PIA.

file as required under the federal rules of evidence,[13] but non-vetted candidate information will not be used for leads or entered in an ROI in ICE systems. The existence of a potential WCH match is not treated by investigators as proof of criminal activity, but rather an investigative lead or tip, requiring further investigation.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

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, as amended (HSA), 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 residing 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 relating to human rights violators and war criminals. Many of the federal criminal authorities apply regardless of U.S. citizenship or alienage.

ICE identifies each collection by data provider and implements the provider's authority to use, retain, and share the information according to the terms of the applicable ISAA, which may include a MOA, MOU, or other formal data sharing policy. WCH enables sharing with authorized users after the data provider has approved the sharing through an approved ISAA and as described in SORNs.[14]

The War Crimes Hunter relevant immigration authorities include:

- *Persecution*: 8 U.S.C. § 1158(b)(2)(A)(i) [asylum]; 8 U.S.C. § 1231(b)(3)(B)(i) [withholding of removal]; 8 U.S.C. § 1101(a)(42)(B) [refugee definition];
- *Genocide:* 8 U.S.C. §§ 1182(a)(3)(E)(ii), 1227(a)(4)(D);

[13] *Available at* https://www.rulesofevidence.org/.
[14] See Appendix A for additional information.

- *Particularly Severe Violations of Religious Freedom:* 8 U.S.C. §§ 1182(a)(2)(G), 1227(a)(4)(E);
- *Torture:* 8 U.S.C. §§ 1182(a)(3)(E)(iii)(I), 1227(a)(4)(D);
- *Extrajudicial Killing:* 8 U.S.C. §§ 1182(a)(3)(E)(iii)(II), 1227(a)(4)(D); and
- *Recruitment or Use of Child Soldiers:* 8 U.S.C. §§ 1182(a)(3)(G), 1227(a)(4)(F).

The War Crimes Hunter related criminal authorities that are applicable to U.S. persons and aliens include:

- *Genocide*: 18 U.S.C. § 1091;
- *Torture*: 18 U.S.C. § 2340-2340A;
- *War Crimes*: 18 U.S.C. § 2441;
- *Use or Recruitment of Child Soldiers*: 18 U.S.C. § 2442; and
- *Providing Material Support to* [Torture, Genocide, Use/Recruitment of Child Soldiers]: 18 U.S.C. § 2339A.

Additionally, ICE operates the WCH system to support partner agencies, which carry out their authorities pursuant to applicable law and regulation. Specific authorities are referenced in applicable privacy compliance documentation listed in Appendix A, updated as appropriate.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information collected by WCH is covered by the DHS/ICE-009 External Investigation SORN.[15] ICE is publishing an update to the SORN to provide additional transparency to the collections by WCH.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

WCH falls under the security environment for HSI's Repository for Advanced Analytics in a Virtualized Environment (RAVEn).[16] RAVEn is a cloud-based environment for HSI and serves as a curation point for data analytics and data analytic tools. RAVEn's system security plan was approved when it secured an Authority to Operate on September 17, 2019. RAVEn will undergo a review of its security plan every three years.

[15] DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010). An update to the SORN providing notice to HSI's use of facial biometrics is forthcoming.
[16] *See* DHS/ICE/PIA-055 Repository for Advanced Analytics in a Virtualized Environment (RAVEn) *available at* www.dhs.gov/privacy.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Records relating to WCH are retained for 75 years after the initial collection in accordance with DAA-0563-2013-0001-0006.[17] This DHS-wide biometric schedule applies to photographs collected for the identification, investigation, apprehension, and/or removal of aliens unlawfully entering or present in the United States. An updated schedule for investigative records will be developed by ICE and submitted to NARA for approval.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

WCH does not collect information directly from the public and therefore is not covered by the PRA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

WCH's purpose is to capture and preserve media depicting human rights violations/violators and acts indicative of war crimes being committed outside of the United States. Since the identity of the violator is unknown to HRVWCU at the time of collection, it is not possible to immediately determine if an individual is a U.S. person (a U.S. citizen or Lawful Permanent Resident). As such, all images are handled in accordance with the Privacy Act as well as DHS and ICE policies regarding the safeguarding and dissemination of PII. Bystanders or victims depicted in the data may initially be collected by WCH but will be blurred in the media retained in the WCH repository. WCH will isolate and extract faces of violators from the media for querying against databases run by partner agencies. WCH will assign a unique identifier to each isolated face image to associate the image with the collected source data. WCH will indicate the statutory violation(s) that applies to each suspected human rights violator whose image is captured.

If a partner is able to create a candidate list of potential matches based on a minimum score, it might return, or provide access to, the following information from its databases:

- Name;

[17] *Available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

- Date of birth;
- Corresponding facial images;
- Unique identifiers assigned by the partner (e.g., Fingerprint ID number);
- Information related to the partner's encounter with the candidate;
- Derogatory information that may be associated with the candidate; and
- When available, confidence level scores of the match created by the partner's processes.[18]
    - *Confidence levels are not indicative of any criminal activity, but rather explains the likelihood of a match following analysis by a trained facial examiner.*

2.2 What are the sources of the information and how is the information collected for the project?

WCH will collect media from open source content available to the public at large via the internet. The websites from which WCH will collect media are freely available to any member of the public and are maintained by a variety of entities including individuals or organizations engaged in human rights violations (perpetrators); journalists; international organizations; and human rights organizations. The WCH tool will be used to scrape media from websites or third-party aggregators which might include social media posts from individuals.

WCH images may match against information about a known individual in partner agency biometric databases. This information may have been obtained by partners directly from the known individual, or through indirect means pursuant to a law enforcement or national security purpose. More information on the sources of agency partner information can be found in the respective privacy documentation cited in the appendix(s) to this PIA.[19]

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

As noted above, WCH will retrieve publicly available media from publicly accessible websites, blogs, or aggregators. These sources may contain social media posts from individuals. Information retrieved by WCH will be for the purpose of collecting images which may be used to

[18] A full listing of potential data elements returned by each agency partner is listed in the appendix(s) of this PIA. For more information about a partner's processes or scores, *see* the privacy compliance documentation cited in each appendix.
[19] *Id.*

identify individuals suspected of potential war crimes or human rights violations. All collections by WCH are only used to generate leads or tips for further investigation by HSI.

2.4 Discuss how accuracy of the data is ensured.

HRVWCU will only designate a website for ongoing collection by the WCH tool if, after thorough research and investigation, the site is deemed relevant and credible by a HRVWCU supervisor. HRVWCU will vet a site against HSI data holdings and other research to determine credibility. HRVWCU will also confirm that media present on the site contains potential war crimes or human rights violations before facial images are isolated and collected.

WCH users will choose isolated images, derived from the media collected, that most closely approximate "constrained images," in that the angle, distance, lighting, and quality that is present in the image resembles traditional mugshots and visa photographs. WCH users will refine their isolation techniques through consultation with the partner agency biometric subject matter experts. This practice will endeavor to reduce any sources of potential errors or false matches from facial recognition technology.

The accuracy of the facial recognition technology used by the agency partner is the responsibility of the partners. However, HRVWCU will partner with agencies having biometric databases for which the agencies have provided adequate privacy compliance documentation, such as PIAs, explaining the systems' processes and risks. HRVWCU will also ensure that agency partners use facial examiners to review candidate lists of image returns. Examiner review provides a manual evaluation of the accuracy of the candidate list.[20]

HRVWCU relies on its partner agencies, who originally collected the biographic and encounter data, to provide accurate information in response to images submitted by HRVWCU. Information about candidates returned by partner agencies is assumed to be accurate because the personally identifiable information, including biometric identifiers such as fingerprints and images, was collected directly from the individual to whom it pertains. The original collection of the data by agency partners will also be for a law enforcement or national security purpose. Inaccurate law enforcement records limit a partner's mission effectiveness and compromise criminal prosecutions. Therefore, partners have strong self-interest and incentive to ensure that their data is as accurate as possible before updating their systems. Moreover, all partners are required by the Privacy Act to maintain relevant, timely, and complete records.[21] Finally, individuals are allowed to access and correct information that was not collected for law enforcement or national security purposes through each individual partner's redress procedures.[22]

[20] Partner facial recognition processes are detailed in the appendix of this PIA.
[21] *See* 5 U.S.C. § 552a(e)(5).
[22] For more information on redress procedures for each partner, *see* the appendices of this PIA.

Information received by WCH, either from open source systems or partners, will be vetted by HRVWCU for corroborating evidence before any enforcement action is taken. Possible facial matches are considered investigative leads until additional evidence either validates or eliminates the potential match. Additional evidence leading to validation or elimination includes: biographic information, current and previous addresses, telephone numbers, registered vehicle information (including license plate numbers), criminal history, immigration history, and social media. All information, including social media collections, will be treated as a lead or tip and will not be used to determine an individual's eligibility for an immigration benefit or used as sole proof of criminal activity. After the vetting process, a subject matter record will be created in ICM regarding the subject. Only if the information is deemed to be actionable will the information will be forwarded to HSI field investigators or law enforcement partners for further investigation. HSI field agents will then pursue WCH leads with the same processes used in traditional investigations to determine if a lead is accurate before initiating any enforcement action.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the WCH collection tool may violate privacy settings placed by an individual on his/her social media accounts.

Mitigation: This risk is mitigated. HRVWCU will only access and research publicly available websites prior to setting the WCH tool to start automated collection on a site. HRVWCU will not initiate ongoing collections on any social media platforms where an individual may vary their privacy settings. The WCH tool passively collects media and does not have the capability to "follow," "friend," or "like" an individual's social media account. The tool cannot communicate with an individual in any way and cannot incentivize any site or person to post content or permit access to protected content.

Privacy Risk: There is a risk that WCH will collect information that is considered protected speech under the First Amendment.

Mitigation: This risk is partially mitigated. The Privacy Act generally prohibits the collection of records describing how an individual exercises rights guaranteed by the First Amendment. There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity."[23] HRVWCU personnel receive social media training, in which they are given instruction from the ICE Privacy Division on how to identify First Amendment activity and determine if publicly available content discusses protected activities. ICE personnel manually review all media collected by WCH to determine the accuracy of information, relevance to the WCH mission, and whether it contains protected speech.

[23] 5 U.S.C. § 552a(e)(7).

Privacy Risk: There is a risk that information collected by WCH from open source sites will be inaccurate and unverifiable.

Mitigation: The risk is partially mitigated. HRVWCU will verify a website's credibility via other sources of information prior to designating it for collection by the WCH tool. HRVWCU does not have the technical capacity to analyze all media collected to determine whether it has been digitally manipulated (i.e., "deep fakes"). However, HRVWCU will use traditional investigative methods to vet the veracity of any media prior to generating a lead. The media collected by WCH will not be used to determine benefit eligibility, nor will it be used for establishing probable cause in an investigation. Media collected by the WCH tool will be considered investigative leads until additional evidence either validates or refutes what was collected.

Privacy Risk: There is a risk that WCH will collect information that is not relevant for investigating and prosecuting human rights violations or war crimes.

Mitigation: The risk is mitigated. HRVWCU will verify a website's relevance to the investigation of war crimes and human rights violations prior to designating the site for ongoing collection by the WCH tool. If WCH gathers media that does not depict human rights violations or war crimes, that data will be purged by WCH users upon identification. If WCH gathers media that depicts criminal activity outside the investigative authorities of HRVWCU, the media will be passed to the unit or agency with the authority to review that data in accordance with ICE information sharing standards and practices. For example, if the WCH tool inadvertently collects child exploitation images from a pre-designated website, HRVWCU will send that media to ICE's Child Exploitations Investigation Unit for further investigation. All traditional safeguards for handling and transferring such information will be made and noted in an ICE case management system. The media will then be purged from WCH.

Privacy Risk: There is a risk that WCH will collect information on individuals who are not suspected of human rights violations or war crimes.

Mitigation: This risk is partially mitigated. Any images irrelevant to the identification of war criminals or human rights violators will be purged from the system. There are also mitigation strategies in place to ensure no witness or non-participant is inadvertently shared, including a capability to blur faces in the original media and a process that requires WCH users to manually isolate perpetrator images and review each face image before sharing with partners.

Privacy Risk: There is a risk partners will misidentify individuals in the facial recognition process. This risk is increased because ICE does not have control over the accuracy standards or thresholds set by partner recognition technologies.

Mitigation: The risk is partially mitigated. WCH partner technologies will return lists of candidates rather than making positive identifications of a single individual. Those lists will be

verified by partner facial examiners who are trained to compare facial images, thereby reducing any effect inaccuracies or bias within a technology may have regarding identification and reducing any disparate impact on communities that may result from inaccuracies or bias. Further, final candidate lists returned by a partner to HRVWCU will not be used for any law enforcement action without additional research and analysis. WCH users will cross check partner returns against government databases and open source information, such as news articles or Non-Governmental Organization reports, 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 retaining the facial biometrics for juveniles may result in inaccurate results due to factors including growth and aging.

Mitigation: This risk is partially mitigated. The WCH tool will collect media regardless of the age of individuals depicted in the content. HRVWCU treats juvenile human rights violators on a case by case basis, but must first determine the age of the individual, which is difficult to do from an unidentified image alone. For cases in which an individual is identified as a juvenile (15 and under) HRVWCU consults with ICE attorneys prior to submitting the images to a partner. All WCH partners use facial examiners to check candidate lists returned by the facial recognition technology. These examiners are trained regarding the effects of aging and are trained on how to compare images that contain two differently aged individuals.

Currently, the effects of aging on the algorithmic process has been shown by NIST testing to increase the rate of "false negatives" rather than "false positives" in an algorithmic search.[24] Aging causes an algorithm to become less confident the individual in a submitted image is the same individual retained in its gallery, but it does not cause the similarity score for other individuals to increase. This means if HRVWCU submits juvenile facial images from old media or a partner retains a WCH image for an extensive period, it will not increase the chances an individual is incorrectly matched to a WCH collection. WCH partners are constantly refining and improving their facial matching algorithms to increase accuracy and reduce the effects of aging. As individuals grow older at a relatively slow rate, partners have time to improve the accuracy of their algorithmic matching processes.

Privacy Risk: There is a risk that WCH will receive and use inaccurate biographic or encounter information received from partners.

Mitigation: This risk is partially mitigated. HRVWCU will rely on biographic and encounter data returned by agency partners to be accurate because the data is associated with other biometric identifiers, such as a 10-print fingerprint scan. Associating data with a biometric identifier ensures the original data collection by the partner is tied to an unchangeable individual

[24] *See* NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, pg 7 *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

attribute, as opposed to a name or assigned numeric identifier. It also reduces the incidences of human error (i.e., transposing numbers or misspelling names) and eliminates instances of associating information with an individual who has similar information, such as the same name or date of birth. The original collection of the data by agency partners will be either from the individual directly or collected for a law enforcement or national security purpose, increasing the likelihood that the information has been vetted for accuracy by another federal agency. WCH partner agencies are also required by the Privacy Act to ensure records within their systems are as current and accurate as possible.[25] All WCH partners have processes to allow an individual to access and amend information within their systems.[26] Additionally, HRVWCU will conduct its own research and investigation to determine if the information returned by a partner is accurate before taking any enforcement action.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

WCH will collect media from publicly available websites for the purpose of documenting war crimes and/or human rights abuses and identifying potential human rights violators and/or war criminals. WCH will isolate the facial images of unknown individuals believed to be perpetrators of a war crime or human rights abuse to send to partners, who will compare the facial images against photo images in their databases via facial matching technology. Partners may use the images provided by WCH for their own law enforcement purposes in accordance with their authorities and information sharing agreements. An explanation of permissible uses by each partner is outlined in the relevant appendix of this PIA.

Partners will return a list of potential matches to HRVWCU, which will include matching facial images and could also include: biographic information, a description of the encounter in which the partner came to possess the individual's biometric information, and derogatory information contained within the partner's biometric database. HRVWCU will vet information received from the partner against HSI data holdings to corroborate likelihood of an identity match. If a candidate identity is properly corroborated, the information is entered into the ICM as either a subject record for review by DHS and/or the Department of State when a subject applies for an immigration benefit,[27] or a report of investigation which is sent to an HSI field office for investigation and follow up. At no time will HRVWCU use information it collected via WCH or

[25] *See* 5 U.S.C. 552a(e)(6). The Privacy Act only covers individuals who are U.S. Citizens and Lawful Permanent residents.
[26] Access and correction of records may be limited for law enforcement and national security systems. *See* the appendix(s) of this PIA for further details on partner agency access and redress.
[27] For more information on subject records *see* DHS/ICE/PIA-045 ICM *and* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing *available at* www.dhs.gov/privacy.

received from its partners as the sole evidence to recommend that an agency deny immigration benefits to an individual or as proof of criminal activity.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The WCH tool will not be used to discover or locate predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

No other DHS component or partner has access to WCH.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: ICE may inappropriately use information collected or received by WCH.

Mitigation: The risk is mitigated. User roles and access controls are incorporated into WCH so that only users with a need to know can access the tool or the collected media. Any HRVWCU personnel involved in the collection, processing, vetting, or sharing of WCH data will be required to undergo training (such as social media training) on the appropriate uses of data collected by the WCH program and received from partners. Personnel will receive access only after satisfactory completion of the training and with approval from an HRVWCU supervisor. Anyone who is found to have used the system in an unauthorized manner will be disciplined in accordance with ICE policy and/or federal law.

Privacy Risk: Partner agencies may use images collected by WCH for purposes other than the original purpose of collection.

Mitigation: The risk is partially mitigated. The partner agencies that HRVWCU engages with for its WCH efforts have authorities and missions consistent and compatible with the authorities and mission of DHS, ICE, and HRVWCU. All partners will have established privacy compliance documentation (e.g., a PIA) noting the uses of information within their systems. HRVWCU ensures through the ISAA/ICA process that any use by partner agencies will fall under the scope of HRVWCU work—including law enforcement and national security. All WCH partners will assist HRVWCU in completing privacy compliance documentation that details appropriate uses of WCH data. Both agency partners' privacy offices and attorneys will review these uses. The partners will also assist HRVWCU in updating the appendices in this PIA outlining in detail the partner's use of WCH data.

Privacy Risk: ICE may retain or use information that is on a candidate list but is not about a vetted match individual.

Mitigation: The risk is partially mitigated. Candidate lists are maintained in investigative case files per the federal rules of evidence. The case files are not searched by personal identifier and HRVWCU will not enter any information regarding unvetted individuals into ICM or other searchable systems. The amount of information returned on a candidate list will vary by a partner agency. Information returned by a partner agency is generally not actionable and is already contained within systems that ICE has access to as a law enforcement partner. If HRVWCU receives information from a partner that has actionable intelligence requiring action by ICE or other federal, state, local, or international agency, HRVWCU may share that information outside of HRVWCU after supervisory review. WCH users are trained to vet all information derived from partners for corroboration prior to lead generation or sharing. Recipients of the information would be law enforcement personnel who are trained to handle information pursuant to strict evidentiary standards. WCH will not share information without actionable intelligence with any organizations other than partner biometric databases.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

ICE will not provide an individual notice if WCH collects his or her information from an open source site. WCH collections involve individuals whose identity is unknown to HRVWCU, so WCH is unable to provide notice. Similarly, ICE will not provide notice to an individual if his or her information is returned as a candidate from a partner. Notification following a partner match would jeopardize the ability of HRVWCU to collect further information, follow up on investigations, or carry out a law enforcement action (if necessary) against the individual.

This PIA provides the public notice of the operations and collection methods of WCH. The DHS/ICE-009 External Investigations SORN provides general notice of ICE's efforts to collect and maintain records and information related to inquiries and investigations pertaining to suspected violations of law.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

WCH does not directly collect information from individuals and is used for law enforcement purposes. Individuals, therefore, do not have an opportunity to opt out of WCH

collections. Opt-out procedures for a partner's biometric collection or sharing will be listed in the compliance documentation for that partner and are cited in the relevant appendix of this PIA.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice prior to collection of their information by WCH. This risk is increased because individuals may not be aware that their posts are public or that another individual has posted their information to a publicly accessible site.

Mitigation: This risk is not mitigated. The WCH tool will only collect media from websites that are designated by HRVWCU as publicly available. The tool does not violate any social media account's privacy settings, nor does it engage individuals or groups online to actively procure information (such as "friending" or "liking"). HRVWCU, however, does not have the ability to determine if a website designated for collection received a third party's consent to post information about that individual.

Privacy Risk: There is a risk that partners will not provide adequate notice that their biometric collections may be used for WCH.

Mitigation: The risk is partially mitigated. WCH partners, when possible, collect images and biographic information directly from the individual in conjunction with a fingerprint scan. Individuals at that time are notified that the collections are accomplished either for a law enforcement purpose or for background checks and that their biometrics (notably, fingerprints) will be used for matching purposes and to determine identity.

Privacy Risk: There is a risk that individuals will not have access to images or videos collected by WCH that will be used against them in criminal or immigration proceedings.

Mitigation: This risk is partially mitigated. All individuals present in the United States have constitutional protections in criminal proceedings that entitle them to discovery production.[28] The discovery obligations of federal prosecutors are generally established by Federal Rules of Criminal Procedure 16 and 26.2, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*,[29] and *Giglio v. United States*.[30] With respect to immigration proceedings, each party is responsible for producing any evidence upon which it seeks to rely in the litigation. Therefore, if ICE seeks to use information derived from WCH in support of any charge, it would produce that information.

[28] Discovery is the general process of a defendant obtaining information possessed by a prosecutor regarding the defendant's case.
[29] 373 U.S. 83 (1963).
[30] 405 U.S. 150 (1972).

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

WCH will retain evidence of human rights violations and war crimes for 75 years after original collection, in accordance with a DHS-wide biometrics retention schedule, DAA-0563-2013-0001-0006. There is no statute of limitations on war crimes or human rights violations. Therefore, if a subject of an investigation were to attempt to enter the United States at any time after a WCH collection, ICE would still retain this information, as it may be vital to ICE's law enforcement mission. If a partner does not have the capacity to retain unidentified images in their respective databases, the WCH images will be immediately deleted after a query. Otherwise, the retention schedule will follow the images as they are submitted to partners and ICE will update partners as to when images should be deleted.

Agency partners may use shared WCH collections pursuant to their applicable authorities (i.e., the FBI may use a WCH collection as a lead in a counterterrorism investigation). Any information that are retained by partners for their own use may be kept longer than the retention period identified above. The records retention schedule(s) of each partner is discussed in the appendix(s) of this PIA. Any ongoing cases that may result from WCH will follow the retention schedule of the case management system that contains the records, such as ICM.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk WCH will retain information longer than is relevant or necessary to accomplish its mission.

Mitigation: This risk is partially mitigated. WCH information retention periods are consistent with DHS-wide biometric retention periods and are only held for as long as necessary to support the agency's mission. Images are tagged with a deletion date when entered into the WCH repository. The WCH System Administrator is responsible for reviewing, deleting, or archiving information in accordance with the retention schedule and security controls will be in place to ensure that information is protected during this time.

Privacy Risk: There is a risk partners will retain information longer than is necessary for the WCH mission.

Mitigation: The risk is partially mitigated. WCH's business requirements for its partners, along with this PIA, govern partner retention practices. HRVWCU will ensure, either through an ISAA or interconnection agreement, that the 75-year retention period is observed by partner agencies. HRVWCU will follow up with partners to ensure that collections are deleted in accordance with its schedule. Similarly, HRVWCU will only share WCH collections with partners that have privacy compliance documentation noting the applicable retention schedule. In instances where a partner retention schedule would govern a partner's ongoing use of WCH collection, the

partner will be required by law and governmental policy to destroy the records at the appropriate deletion date.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Sharing images with WCH partners

The primary purpose of WCH is to collect images of suspected war crimes perpetrators and human rights violators and to share those images with partner biometric databases for lead development. WCH will send isolated face images to its Partners using secure communications channels. Different biometric repositories may require pass-through connections via different ICE or DHS systems. Any new system pass-through will be discussed in detail in the relevant partner's appendix of this PIA. These information-sharing relationships are documented in ISAAs. ISAAs set out the terms for WCH users according to their authorities and mission needs. WCH will include a notation of the statutory violation the violator is suspected of committing and numeric identifiers that link the image to the original WCH collection.

Sharing leads with external agencies

Leads generated from WCH processes may ultimately be shared with federal, state, tribal, local and foreign law enforcement agencies, who may or may not be WCH partner agencies, as well as relevant law enforcement fusion centers with which HRVWCU has pre-existing information sharing agreements. WCH data will be shared if the agency has a need to know and doing so will further U.S. government law enforcement and/or national security efforts; provided that disclosure is consistent with applicable law and agency policies. This sharing is done manually by ICE personnel (e.g., via secure email or file transfer) and not via any system-to-system connections. All external sharing of WCH information will be conducted and documented per the procedures of the relevant case management system (ICM) into which the lead is entered.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing images with WCH partners

WCH will only share images it collects with biometric databases maintained by partner agencies pursuant to an ISAA that sets out the terms for sharing, for the purpose of identifying human rights violators and war criminals. This sharing of law enforcement intelligence will only occur with partners that have a need to know the information to properly fulfill their law enforcement, national security, or administrative mission. Sharing is also necessary for WCH to

obtain information pertinent to an ICE investigation. This is compatible with Routine Uses J and Q of the DHS/ICE-009 External Investigations SORN because the initial collection and sharing of images are both for the purposes of collecting and sharing law enforcement intelligence and investigative information.

Sharing leads with external agencies

WCH leads might be shared with foreign, state, local, and federal partners for the purpose of enforcing and administering laws within ICE's jurisdiction. This sharing is compatible with Routine Uses G, L, O, and S of the DHS/ICE-009 External Investigations SORN.

6.3 Does the project place limitations on re-dissemination?

Sharing images with WCH partners

The WCH partners are all Federal agencies that are subject to the Privacy Act and may only disclose information as described in their governing SORN. Each partner SORN is cited in the appendix(s) to this PIA. Further, any sharing of information by WCH with a partner will be governed by an ISAA agreed to by both parties that will ensure that any re-dissemination and third-party sharing of WCH collections will only be for the purposes of the original collection of the information. Onward sharing of WCH information is discussed in detail in the appendices of this PIA. ISAAs may include Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), Implementing Agreements, or other formalized letters describing the purpose, use, and scope of sharing.

Sharing leads with external agencies

Leads generated by WCH will be referred to other government agencies (including federal, state, local, and foreign agencies) pursuant to pre-existing ISAAs, and those agreements include provisions that require those agencies to only use information for purposes in line with WCH's original collection.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Sharing images with WCH partners

The WCH system logs each transmission to an external partner system in the WCH application that formats images for transfer. WCH logs a unique identifier for each transmission, the date/time of transmission, the external system identifier, an identifier unique to the subject of the image, and an identifier for the media from which the image was originally derived.

Sharing leads with external agencies

Any disclosure of information derived from potential leads created through WCH will be noted in the case management system in which the lead is documented. WCH users are required to complete and retain DHS Form 191, Privacy Act Disclosure Record, when making any disclosures outside of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Sharing images with WCH partners

Privacy Risk: There is a risk that WCH partners will share WCH information with other agencies that do not have a need to know.

Mitigation: This risk is mitigated. Any information shared with partners is controlled by the provisions of an ISAA (either a MOU, MOA, or other data-sharing agreement) or Interconnection Agreement. The agreement states that individuals who receive information from WCH may not further disseminate data unless they have prior approval through the ISAA or from ICE. Any potential matches made against WCH images within the biometric databases by a third party will alert the partner to contact HRVWCU. As WCH only transmits images and administrative identifiers to partners, it is necessary for any third party using the partner database to contact HRVWCU directly to attain any derogatory or investigative data pertaining to the image.

Sharing leads with external agencies

Privacy Risk: There is a risk that HRVWCU will share WCH collections prior to properly vetting the data or with organizations that do not have a need to know.

Mitigation: The risk is partially mitigated. The WCH program is designed to identify individuals for pursuing law enforcement or administrative action. If media collected by the WCH tool has actionable intelligence requiring action by a federal, state, local, or international agency, HRVWCU may share that media after supervisory review. WCH users are trained to vet all evidence obtained by the WCH tool to verify its credibility and all data will be corroborated prior to sharing. Recipients of the information would be law enforcement personnel who are trained to handle information pursuant to strict evidentiary standards. WCH will not share collections without actionable intelligence with any organizations other than partner biometric databases. All WCH users will be trained accordingly and have HRVWCU Supervisor permission to be involved with the WCH program.

Further, all leads are reviewed by an HRVWCU agent, analyst, and an ICE attorney prior to HRVWCU sending a lead to the field. HRVWCU personnel are trained on the appropriate sharing of PII and are instructed to contact the ICE Privacy office if they are not sure whether information sharing is appropriate. They must log all leads sent in an ICE case management

system, which uses audit logs to track information shared with external parties. This way, the program can track disclosures and ensure that information is being shared consistent with the provisions of this PIA and DHS/ICE-009 External Investigations SORN.

Privacy Risk: There is a risk that information for individuals designated as members of a Special Protected Class (SPC)[31] will be shared inappropriately.

Mitigation: This risk is partially mitigated. WCH users cannot verify whether unidentified individuals are members of a SPC, and information returned by a partner agency on candidate lists will vary by agency. DHS policy requires that all Component systems and programs with access to SPC information must establish a mechanism for identifying individuals with a protected status. WCH users will check the DHS IDENT system[32] for an individual's biographic information prior to generating a lead. Any applicant for SPC status must submit information that is ingested by IDENT on a daily basis, and IDENT provides users with an alert message to indicate when an individual is protected by 8 U.S.C. § 1367 or by another SPC status. This makes IDENT users immediately aware that they are displaying a record relating to a protected individual and that specific procedures regarding the disclosure and use of the information apply. Any record in IDENT that displays this banner must be handled in accordance with the all laws, regulations and DHS policy.[33] WCH users are trained to recognize the IDENT warning banner and the proper handling of SPC information, including its restrictions on sharing.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

WCH image collections will not initially contain biographic information that identifies the individual. As such, it is not possible to retrieve information from the WCH collections based on the identity of the individual depicted. Any information retained in partner agency databases must be accessed via that partner's own redress processes. Those processes are detailed in the appendix(s) of this PIA. After potential matches are returned from a WCH partner, information may be entered into ICM, and redress procedures will follow those systems' parameters.

---

[31] *See* 8 U.S.C. § 1367 Penalties for unauthorized disclosure of information of special protected classes.
[32] *See* DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy.
[33] *See* DHS Directive 002-02, Revision 00.1, *Implementation of Section 1367 Information Provisions* (Apr. 29, 2019), and Instruction 002-02-001, *Implementation of Section 1367 Information Provisions* (Nov. 7, 2013), provides general policy and guidance on disclosure of Section 1367 information, including the VAWA's eight statutory exceptions to the general nondisclosure requirement. All other sharing of personally identifiable information (PII) to third parties must be consistent with Department policy, including DHS's privacy policies and information sharing policies.

U.S. citizens, lawful permanent residents, and covered individuals who have covered records under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information. All individuals, regardless of citizenship, may obtain access to records consistent with the Freedom of Information Act (FOIA) unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Individuals seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE FOIA officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be irretrievable (as stated above) or exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As stated above, initial WCH collections will not have personally identifiable information attached to the individuals in images or videos, and therefore there are no procedures for correcting information in the WCH repository. Individuals seeking to correct records associated with WCH leads contained in the ICM system of records, or seeking to contest its content, may submit a request in writing to the ICE Privacy and Records Office by mail:

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

All or some of the requested information may be exempt from correction pursuant to the JRA or Privacy Act in order to prevent harm to law enforcement investigations or interests.

Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

7.3 How does the project notify individuals about the procedures for correcting their information?

ICE provides general notice on its public-facing website about the procedures for submitting Freedom of Information and Privacy Act requests. Notice of redress procedures is also contained in this PIA and the DHS/ICE-009 External Investigations SORN. No individual notification of procedures for correcting WCH records is currently provided, however. WCH contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notification to individuals that they are or have been the target of a law enforcement investigation could undermine the law enforcement mission of ICE.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals won't be able to access and amend inaccuracies in WCH collections.

Mitigation: This risk will not be mitigated, as initial media collections by the WCH tool are unidentifiable, and therefore will not be able to be retrieved within the system by personal identifier. The WCH tool collects media from publicly available sources, and an individual's correction of information or other updates in open sources will not notify or update WCH. Individuals identified as potential human rights violators via WCH data will 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, civil, or regulatory 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, and to avoid detection or apprehension.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

ICE ensures compliance with this PIA by instituting rigorous standards for training, rules of behavior, information sharing, auditing, and supervisory oversight. Additionally, the Rules of Behavior (ROB) for WCH have been created in consultation with the ICE Privacy Division and

ICE attorneys to ensure the practices protect the privacy and civil rights and civil liberties of individuals and align with this PIA. The ROB is signed by all WCH users collecting the media. All WCH users are also trained on appropriate use of social media by the ICE Privacy Division before accessing social media and are trained annually thereafter. HRVWCU supervisors are required to monitor and approve which sites are designated for WCH collections, who designated those sites, and what images are sent to WCH partner biometric databases. A log file containing this information is available to the HRVWCU supervisors in order to conduct a complete audit. Any WCH user found to be using social media or the WCH tool for an inappropriate purpose will have his/her access revoked.

External connections are documented and approved with both parties' signatures in an ISAA, which outlines controls in place to protect the confidentiality, integrity, and availability of the information being shared or processed.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All HRVWCU personnel are required to take annual privacy and security training, which emphasizes general ICE ROB required to access any DHS system and other legal and policy restrictions on user behavior. Additionally, all HRVWCU personnel that access social media are required to take annual privacy training on the operational use of social media and WCH's specific ROB. WCH users will also be required to take system-specific training on appropriate uses of the tool as part of HRVWCU's operations training. HRVWCU supervisors track personnel completion of training and will not grant system access until a user's training is complete.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only ICE personnel whose official duties necessitate access to WCH will be granted access. HRVWCU management oversees and approves the assignment of user accounts to ICE personnel. Access roles are assigned by a supervisor based on the user's job responsibilities. Access roles are reviewed regularly to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list. The minimum requirements for access are documented in the ISAAs between and among DHS and specific users, and in security, technical, and business documentation.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All new information sharing agreements will be reviewed by the program's Information Systems Security Officer, the ICE Information Governance and Privacy Division, the Office of the Principal Legal Advisor, key program stakeholders, and the Program Manager. The ISAA will then be sent to DHS for formal review. ICE Memoranda of Understanding (MOUs) clearly articulate who will be accessing the shared information and how it will be used and are reviewed and approved by DHS oversight offices, including the DHS Privacy Office. If the terms of existing MOUs are changed, addendums will be established and reviewed in the same manner as described above.

Responsible Officials

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

Approval Signature

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

_____
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

Appendix: A

Organization:

DHS Office of Biometric Identity Management (OBIM)

Purpose and Use:

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.[34] OBIM is undertaking a modernization program by deploying the Homeland Advanced Recognition Technology (HART) system to replace IDENT. 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 the Department. As a data steward, OBIM provides a service to its data providers and data users. OBIM identifies each collection by data provider and its authority to use, retain, and share data. IDENT enables sharing with authorized users after the data provider has approved the sharing.

WCH will connect to IDENT/HART directly through the ICE Repository for Analytics in a Virtualized Environment (RAVEn).[35] After IDENT/HART accepts a WCH transmission, it will vet WCH images against current DHS holdings of biometrics to generate investigative leads. IDENT/HART will also store WCH images and check WCH images in later searches requested by other users. OBIM sharing will make biographic, biometric, and derogatory information of potential suspect matches available to HRVWCU to vet as a lead. IDENT/HART will store images to alert HRVWCU and OBIM when new IDENT/HART biometric encounters (visa applications, arrests for immigration violations, etc.) enter the system and match a WCH image.

The sharing and search process will be as follows:

- HRVWCU will submit WCH face data to IDENT/HART for a facial 1 to many search against the entire gallery of facial images contained within IDENT/HART;
- The IDENT/HART face matching technology will find a pre-determined number of candidates[36] who have the most similarity to the image submitted by HRVWCU within its galleries. A minimum threshold of similarity will be set to exclude images with little to no similarities.

[34] *See* DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy. HART will be discussed in a forthcoming PIA.
[35] *See* DHS/ICE/PIA-055 RAVEn *available at* www.dhs.gov/privacy.
[36] Currently IDENT/HART will return a candidate list of 20 individuals. The actual number of candidates returned may change as technology and business needs change.

- Trained facial examiners from OBIM's Biometric Support Center (BSC) will review the returns of the search and adjudicate the candidate lists of potential facial matches;
- OBIM will delete WCH images after a query is complete;
- HRVWCU will update OBIM on any identified individuals through traditional case management processes and information will be entered with the established OBIM identity.

Currently OBIM will delete all WCH submissions after a query is complete. OBIM, however, is developing a repository to enroll unknown identities in its system. When this capability is developed OBIM will store WCH face data that does not result in any likely matches within the HART repository of unknown identities, called the Unsolved Face File (UFF), as a new unknown identity. This functionality will not go into effect until OBIM publishes a PIA assessing the privacy risks and mitigations of the UFF. At that point, this appendix will also be updated.

Individuals Searched:

IDENT/HART contains information:

- Directly from the individual applying for a credential, through opt-in enrollments (e.g. Global Entry[37] and TSA Precheck[38]); an immigration benefit, pursuant to a background investigation;
- From intelligence collection conducted to support an authorized intelligence mission;
- Via military and law enforcement direct encounters or forensic operations according to the data provider's authority; or
- Through records shared by foreign governments according to written agreement or cooperative arrangement.

External DHS data providers include Department of State (DoS); Department of Justice (DOJ); Department of Defense (DOD); other federal, state, local, tribal, territorial law enforcement organizations, foreign governments, and international agencies. Foreign government data providers include the Five Eyes/Migration Five Partners, namely Canada, United Kingdom, Australia, and New Zealand, certain Visa Waiver Program (VWP) countries under the Protecting and Combatting Serious Crime Agreements, and other allied nations providing information pursuant to an agreement or arrangement. International agency information can include Office of the United Nations High Commissioner for Refugees

[37] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* www.dhs.gov/privacy.
[38] *See* DHS/TSA/PIA-041 TSA Pre✓™ Application Program, *available at* www.dhs.gov/privacy.

(UNHCR) collected biometrics for refugees who are referred to the United States for resettlement.

DHS data provider sources include the DHS Office of Policy as the Program Manager for information sharing with international partners, Customs and Border Protection, ICE, U.S. Coast Guard (USCG), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA), Federal Emergency Management Administration (FEMA), the DHS Office of the Chief Security Officer (OCSO), and the Intelligence Community. For example:

- The USCG interdicts and refers for prosecution illegal immigrants and migrant smugglers off the coast of the United States;
- USCIS may collect information to establish and verify the identities of individuals applying, and being adjudicated for immigration benefits, including asylum or refugee status; and
- TSA collects information to support the vetting and adjudication of their current credentialing populations which may include workers seeking access to secure facilities, and TSA Precheck applicants.

Relevant Privacy Compliance Documentation:

Privacy Impact Assessments (PIA): DHS/OBIM/PIA-001 Automated Biometric Identification System (IDENT)[39] and DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1.[40]

System of Record Notices (SORN): DHS/ALL-041 External Biometric Records (EBR),[41] and DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records.[42]

Data Elements Accessible by War Crimes Hunter:

- Biometric data, including: facial images, fingerprints, and iris images;
- Biometric-associated biographic data including full name (i.e., first, middle, last, nicknames, and aliases); date of birth (DOB); gender; personal physical details (e.g., height, weight, eye color, and hair color); signature; assigned number identifiers (e.g., A-Number, Social Security number (SSN), state identification number, civil record number, other agency system-specific fingerprint record locator information, Federal Bureau of Investigation (FBI) Number (FNU)/Universal Control Number (UCN), Encounter Identification Number (EID), DoD Biometric Identifier (DoD BID), National Unique

[39] *Available at* www.dhs.gov/privacy.
[40] *Available at* www.dhs.gov/privacy.
[41] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018).
[42] DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records, 85 FR 14955 (March 16, 2020).

Identification Number (NUIN), document information and identifiers (e.g., passport and visa data, document type, document number, country of issuance), when available); and identifiers for citizenship and nationality, including person-centric details (e.g., country of birth, country of citizenship, and nationality, when available);

- Derogatory Information,[43] which may consist of wants and warrants, known or suspected terrorist (KST) designation, sexual offender registration, foreign criminal convictions, and immigration violations, when available. Specifically, the data elements include the following: KSTs, wanted persons, sex offenders, state and local criminals flagged by state/local law enforcement from the FBI; subjects who have violated U.S. immigration laws or who have been denied a biometric visa by DoS; individuals encountered by the DoD during military operations; international criminal data provided by INTERPOL, DoD, FBI, and our international partners; aliens with criminal history, known or suspected gang members, enforcement actions taken at CBP Ports of Entry; expedited ICE immigration removals; and law enforcement community alerts;
- Miscellaneous officer comment information, when available;
- Encounter data, including location and circumstance of each instance resulting in biometric collection; and
- Unique machine-generated identifiers (e.g., fingerprint identification number (FIN), EID, and Transaction Control Number (TCN)) that link individuals with their encounters, biometrics, records, and other data elements. These data elements enable the execution of administrative functions of the biometric repository such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.

Retention by Partner and Permissible Uses:

For identified individuals, IDENT/HART is able to mirror the retention schedule of the users that submit biometrics. Therefore, international WCH images in HART/IDENT will be retained for 75 years after collection by WCH. ICE will notify OBIM after the 75-year retention has expired. OBIM, through the Delete Encounter service, allows data owners to schedule the deletion of biometric records in accordance with their NARA-approved retention schedule. Data owners, however, may need to recalibrate retention schedules in consideration of the different types of biometric identification. DHS is re-evaluating the current retention policy to determine whether a new retention period or combination of retention periods is appropriate. DHS will publish a PIA update for any change in the retention period.

[43] Each IDENT/HART user may use authorized DI received from a IDENT/HART response in accordance with mission needs and as defined in ISAA or as defined in DHS component compliance documentation.

Currently, OBIM will delete all unidentified facial images after a query is complete. When the UFF functionality is developed and the OBIM PIA that assesses the UFF is published, OBIM will retain WCH images that are not initially identified for future searches against known images to support the DHS mission. Images submitted by IDENT/HART users from individuals whose identities are known will be searched against the UFF to determine if there is a match...

As WCH does not include any other PII with WCH images (besides suspected grounds of inadmissibility), any potential match made against WCH images in IDENT/HART's UFF will only alert an IDENT/HART user to contact HRVWCU for follow up. A potential match of a user's submission to WCH images will not, by itself, lead to arrest, detention, or denial of benefits by any user of IDENT/HART.

OBIM's current Record Schedule DAA-0563-2013-0001 covers DHS biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities has been approved by National Archives and Records Administration (NARA). EBR records include:

- Law Enforcement Records: Identification, investigation, apprehension, and/or removal of aliens unlawfully entering or present in the United States and facilitate legal entry of individuals into the United States, which must be destroyed or deleted 75 years after the end of the calendar year in which the data is gathered.
- Records related to the analysis of relationship patterns among individuals and organizations that are indicative of violations of the customs and immigration laws including possible terrorist threats from non-obvious relationships and specific leads and law enforcement intelligence for active and new investigations. These records must be destroyed or deleted 15 years after the end of calendar year of last use of individual's data.

Onward Transfer:

OBIM shares information as permitted with other OBIM users in accordance with the user's authorities. Authorities and access will be determined by OBIM when the user requests access to the system through an Information Sharing and Access Agreement (ISAA). Information may be shared with federal agencies, state, local, tribal, and territorial law enforcement agencies, and foreign and international agencies for national security, law enforcement, criminal justice, immigration screening and border management, intelligence purposes, and national defense as well as to conduct background investigations for national security positions, credentialing, and certain positions of public trust consistent with applicable DHS authorities. Potential matches to WCH images by OBIM users (external or DHS) will only result in an alert to the OBIM BSC to contact HRVWCU for follow up.

Correction and Redress:

U.S. citizens and lawful permanent residents, as well as other persons with records covered by the Judicial Redress Act (JRA)[44] may seek access to their records and to amend inaccurate records by filing a Privacy Act amendment request under the Privacy Act. Those individuals covered under by the JRA or Privacy Act may direct all requests to contest or amend information to the OBIM Privacy, Department of Homeland Security, 245 Murray Drive SW, Washington, DC 20598-0675. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, and the proposed amendment.

If an individual is dissatisfied with the response to his or her redress inquiry, then he or she can appeal to the DHS Chief Privacy Officer, who reviews the appeal and provides final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted by fax: 1-202-343-4010 or mail at the following address:

Chief Privacy Officer
Attn: DHS Privacy Office, Department of Homeland Security
Mailstop 0655, 245 Murray Lane
Washington, DC 20528

As with access, amendments may be limited pursuant to applicable Privacy Act exemptions asserted by the Department of Homeland Security for the IDENT/HART system.

Additionally, travelers who wish to file for redress can complete an online application through the DHS Traveler Redress Inquiry Program (DHS TRIP)[45] at https://trip.dhs.gov, or mail or email a completed copy of DHS Form 591, Travel Inquiry Form (TIF). For more information about the types of services DHS TRIP can provide, please visit https://www.dhs.gov/step-1-should-i-use-dhs-trip.

Completing the form online saves processing time and helps prevent data entry errors. After an individual submits a redress form, the individual will receive notification of receipt from DHS TRIP. DHS TRIP will review the redress form and will determine which component/agency will be able to respond most effectively to the submission. When a redress request is related to records maintained in HART, DHS TRIP will coordinate with OBIM. OBIM will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request.

[44] For more information *see* the Department of Justice's Office of Privacy and Civil Liberties overview of the Judicial Redress Act *available at* https://www.justice.gov/opcl/judicial-redress-act-2015.
[45] *See* DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* www.dhs.gov/privacy.

Appendix: B

Organization:

Department of Defense (DoD) Defense Forensics and Biometrics Agency (DFBA)

Purpose and Use:

DFBA, a component of the U.S. Army's Office of the Provost Marshal General, executes the responsibilities of the Executive Agent for DoD Forensics and Biometrics on behalf of the Secretary of the Army. In this role, DFBA leads, consolidates and coordinates forensics and biometrics throughout the DoD in support of Identity Activities across the range of military operations. DFBA maintains the DoD Automated Biometric Identification System (ABIS).

ABIS supports DFBA's mission of providing a critical end-to-end capability through a defined operations or intelligence cycle to support tactical and operational decision-making to DoD components. This functionality stretches across the full range of military operations for DoD warfighting, detainee operations, intelligence, law enforcement, and security. ABIS is used to accurately identify or verify the identity of an individual by standardizing and comparing captured biometric data to existing sources and scoring the level of confidence of each potential match.[46]

DoD ABIS stores biometric data, such as fingerprint, latent palm print, iris, and facial images; biographic information, such as name, date of birth (DOB), national origin, address, identification numbers (e.g., Social Security number (SSN), serial number), family relationships, and religion; and contextual information such as location of data collection. DoD ABIS may also store additional PII associated with the purpose of the biometric collection. This information can include medical history, military service history, employment history, and law enforcement/national security encounters. ABIS also stores derogatory data that is derived from individuals encountered by the DoD during military operations; and international criminal data provided by INTERPOL, DoD, the Federal Bureau of Investigation (FBI), and international partners.

WCH will connect to ABIS through the ICE Repository for Analytics in a Virtualized Environment (RAVEn).[47] The data will be exchanged in accordance with the DoD Electronic Biometric Transmission Specification (EBTS), or its equivalent successor, which is based on the ANSI/NIST standard.[48]

DFBA will vet WCH images against current DoD holdings of biometrics to generate

---

[46] *See* DOD BIOMETRICS, Department of Defense Directive 8521.01E; *available at* https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/852101E.pdf?ver=2019-04-11-094409-307.

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

[48] ANSI/NIST-ITL 1-2011, 2015 Update (or most recent), Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information. *See* https://www.nist.gov/programs-projects/ansinist-itl-standard.

investigative leads. It will also store WCH images in DoD ABIS so that ABIS can return these images if they are deemed by DOD to be sufficiently similar in future queries by DoD or other stakeholders.[49] DoD will make biographic, biometric, and derogatory information of potential suspect matches available to the ICE Human Rights Violators and War Crimes Unit (HRVWCU) to vet as a lead. Storage of the images in DoD authoritative databases allows for HRVWCU and DoD to be alerted when new biometric enrollments or queries (e.g., from prisoner detentions, foreign national hiring) may be a potential match to WCH images.

The sharing and query process will be as follows:

- HRVWCU will submit WCH face images to DoD ABIS. DoD ABIS will ingest the images for a face-only search against the entire gallery of facial images contained therein;
- The DoD Authoritative Biometric Repository face matching technology will find a pre-determined number of candidates who have the most similarity to the image submitted by HRVWCU within its galleries. A minimum threshold of similarity will be set to exclude images with little to no similarities;
- Trained facial examiners from DoD will review the returns of the search and adjudicate the candidate lists of potential facial matches;
- DFBA, via DoD ABIS, will return any likely face matches to WCH. Multiple candidate returns may be possible depending on the likelihood of a match as adjudicated by the facial examiners. Only confirmed likely subject matches will be returned per submitted face search, along with any sharable associated biographic, encounter, and derogatory information (DI);[50]
- The DoD ABIS system will store WCH face data that does not result in any likely matches within their face database as a new unknown identity; and
- DoD will allow other authorized stakeholders to perform face searches against the WCH data stored in the ABIS face database.

Subsequent matches against WCH images by a stakeholder will alert the DoD and the partner to contact HRVWCU regarding the potential match to WCH data.

ICE will update DoD when a WCH image has been positively identified. Additional information regarding the individual will be entered and associated with either the established DoD ABIS identity or the previously unidentified face record, as appropriate.

---

[49] *See* Onward Transfer section, below.

[50] More than one matching record for an individual may be returned. DoD ABIS is an encounter-based system; therefore, the probe photo may match face records for the same individual as a result of multiple encounters with that individual.

Individuals Searched:

The DoD maintains authoritative biometric data repositories to conduct match, store, and share functions for the DoD mission areas of:

(1) Individuals whose biometric data was collected during DoD military operations or as a part of national security-related operations. This includes bulk collections from interagency or foreign partner repositories; these individuals include known or suspected terrorists, DoD detainees, and other individuals of interest to DoD; or

(2) Individuals affiliated with or seeking to be affiliated with the DoD whose biometric data were obtained for a legitimate, authorized purpose in accordance with applicable law, regulation, and policy.

Relevant Privacy Compliance Documentation:

Privacy Impact Assessments (PIA): Department of Defense Automated Biometrics Identification System (DoD ABIS) (May 6, 2015);

System of Records Notices (SORN): Defense Biometric Identification Records System A0025-2 Provost Marshal General Defense Forensics and Biometrics Agency DoD.[51]

Data Elements Received by War Crimes Hunter:

- Biometric-associated biographic data including full name (i.e., first, middle, last, nicknames, and aliases); DOB; place of birth; gender; ethnicity and/or tribal information; personal physical details (e.g., height, weight, eye color, and hair color); signature; assigned number identifiers (e.g., A-Number, SSN, state identification number, civil record number, internment serial number); family member names and relationship;
- Derogatory Information, which may consist of wants and warrants, known or suspected terrorist (KST) designation, arrest data, gang membership, criminal data, sexual offender registration, foreign criminal convictions, and immigration violations, when available; and
- ABIS encounter information, such as ABIS encounter specific identifier, reason fingerprinted, date fingerprinted, arrest segment literal, fingerprinting agency, geolocation of data capture, personnel type, Transaction Control Number of matching records, ABIS control numbers, and other agency system-specific fingerprint record locator information.

Retention by Partner and Permissible Uses:

DoD collects biometrics of foreign nationals encountered in areas of combat operations. Some of these individuals may be seeking access to and/or employment by U.S. military installations. Other individuals are potential or actual DoD detainees. Military Services and U.S.

[51] 80 Fed. Reg. 8292 (February 17, 2015).

Combatant Commands rely on ABIS to provide timely, accurate, and complete responses indicating whether persons of interest encountered in the field have a prior history of derogatory (e.g., criminal, terrorist) activity to assist in identifying potential threats to U.S. forces and facilities. DoD will use WCH information to help determine if an individual may pose a risk to national security and/or safety of U.S. forces and service personnel.

ABIS will retain images pursuant to DoD ABIS's retention schedule regarding biometrics (DAA-AU-2013-0007),[52] which is currently 75 years. DoD will update ICE when images are deleted or if there is a change in retention schedule.

Since WCH does not include any PII with the collected images (i.e., only suspected grounds of inadmissibility are included), any potential match made against WCH images in the ABIS face database will only alert an ABIS user to contact HRVWCU for follow-up action. A potential match of a user's submission to WCH images will not, by itself, permit any ABIS user to arrest, detain, or deny benefits to an individual.

Onward Transfer:

Authorized DoD users may search against WCH images. Authorized stakeholders include the FBI, the National Ground Intelligence Center, other DHS Components, and other DoD submitters/customers such as all Combatant Commands (CCMDs), U.S. Navy, U.S. Marine Corps, U.S. Air Force, and Defense Intelligence Agency (DIA). These stakeholders use ABIS to identify biometric matches in support of U.S. criminal cases, border control, and intelligence watchlists.

Both agencies acknowledge that data stored on behalf of third parties, or subsequent matches to that data, will not be shared without the consent of the data owner. Potential matches to WCH images by ABIS users will only result in an alert to the user to contact HRVWCU for follow up action.[53]

Correction and Redress:

Individuals seeking access to information about themselves contained in ABIS should address written inquiries to:

Director
Defense Forensics and Biometrics Agency
251 18th Street South, Suite 244

[52] *See* National Archives and Records Administration, Request for Records Disposition Authority, Records Schedule Number DAA-AU-2013-0007, U.S. Department of Defense, Automated Biometric Identification System (ABIS) (2013), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-defense/department-of-the-army/rg-au/daa-au-2013-0007_sf115.pdf.

[53] *See* Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activates, January 2016 Update.

Arlington, VA 22202-3532

The requester should provide full name, current address and telephone number, and signature. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format: If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).' If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).'

Certain ABIS records may be exempt from access and amendment. The U.S. Army's rule for accessing records, contesting contents, and appealing initial agency determinations are contained in Army Regulation 340-21; 32 CFR part 505;[54] or may be obtained from the system manager.

[54] *See* ARMY PRIVACY ACT PROGRAM, Army Regulation 340-21; *available at* https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN13587_R25_22_FINAL.pdf.

Appendix: C

Organization:

Federal Bureau of Investigation (FBI) International Human Rights Unit (IHRU) and Multimedia Exploitation Unit (MXU)

Purpose and Use:

The FBI IHRU's mission is to lead the FBI in utilizing law enforcement and intelligence resources, both domestic and foreign, to hold perpetrators or serious human rights violators accountable under the rule of law. In support of this mission, the IHRU identifies and generates actionable leads targeting known or suspected human rights violators residing in the United States and disseminates those leads to the field for investigation.

The FBI MXU works to process and exploit multimedia content (i.e., still and video imagery) from digital evidence, FBI-owned collections, and consensual collections from across FBI missions. MXU's identification services use their Multimedia Processing Framework (MPF) to host imagery analytics capabilities including a Recognition Framework that performs facial recognition tasks. MXU also supports a wide variety of law enforcement customers. The MXU provides identification services for national security cases derived from, or relying on, sensitive biometric data with handling or classification restrictions that exceed the FBI's Next Generation Identification (NGI) biometric system. Sources of this data are classified.

WCH will provide face images of suspected human rights violators and war criminals for query against the FBI MXU face database to assist in the identification of these suspects and to augment the holdings of MXU for subsequent queries for intelligence purposes. The goal of this sharing is to vet WCH images against current FBI classified biometric holdings to generate investigative leads and to store WCH images in MXU's database to be queried at a later point.

Prior to transmission of images to MXU, HRVWCU personnel will contact IHRU. The IHRU will review all proposed WCH submissions to understand potential human rights/war crimes violations and the source of information to determine if the FBI has authority and jurisdiction to collect the information.

WCH will connect to FBI/MXU directly through the ICE Repository for Analytics in a Virtualized Environment (RAVEn) for transfer of images.[55] This interface will occur via an unclassified secure connection developed by the FBI. The RAVEn/WCH to MXU electronic interface is one-way. Because the MXU system holds classified data, the FBI does not automatically share any data back with WCH. Rather, this is handled manually through IHRU using other channels (e.g., secure email or secure telephone).

[55] *See* DHS/ICE/PIA-055 RAVEn, *available at* www.dhs.gov/privacy.

After the MXU system accepts a WCH transmission, it will vet WCH images against current MXU holdings of face biometrics to generate investigative leads. MXU will also store WCH images within MXU systems to check WCH images in later FBI internal queries and searches requested by other intelligence community users. MXU will notify IHRU of any matches. IHRU will then determine what information of potential suspect matches can be shared with HRVWCU. MXU will store images and alert IHRU when new biometric data enters the system and matches a WCH image. IHRU will then contact HRVWCU with any shareable information associated with the potential match.

The sharing and query process will be as follows:

- HRVWCU will submit WCH images to IHRU. IHRU will review proposed submissions to confirm that the FBI has sufficient predicate and authority to query and retain the facial images;
- After gaining IHRU concurrence, HRVWCU will submit WCH face data to FBI MXU via RAVEn. FBI MXU will ingest the images into their recognition framework for a 1:many face-only query against the entire gallery of facial images contained therein;
- Trained facial examiners from MXU will review the returns of the query and adjudicate the candidate lists of potential facial matches;
- MXU will return the results of facial recognition processes conducted on WCH images, including biographic and criminal information stored in FBI systems, to IHRU;
- IHRU will determine what information can be shared with HRVWCU. If approved, IHRU will forward any shareable information to HRVWCU through proper channels;
- The MXU system will store WCH face data that does not result in any matches within their face database as a new unknown identity;
- MXU will allow other stakeholders to perform face queries against the WCH data stored in the MXU face database. Subsequent matches against the WCH data will alert the FBI MXU and the partner to contact HRVWCU, through IHRU, regarding the potential match to WCH data; and
- ICE will notify IHRU when a WCH image has been positively identified through its traditional case management process. Additional information regarding the individual will be entered and associated with either the established MXU identity or the previously unidentified face record, as appropriate.

This process does not change or increase the privacy risks to the collection, maintenance, or dissemination of PII that was assessed in the main body of this PIA.

Individuals Searched:

The FBI MXU face database contains information on individuals received:

- From intelligence collections conducted to support an authorized intelligence mission;
- Via military and law enforcement direct encounters or forensic operations according to the data provider's authority; or
- Through records shared by foreign governments according to written agreement or cooperative arrangement.

External MXU data providers include intelligence agencies, other federal, state, local, tribal, territorial law enforcement organizations, foreign governments, and international agencies. Foreign government data providers include signatories of the United Kingdom-United States of America Agreement (Five Eyes),[56] namely Canada, United Kingdom, Australia, and New Zealand; and other allied nations providing information pursuant to an agreement or arrangement.

Relevant Privacy Compliance Documentation:

Privacy Impact Assessments (PIA): MXU's biometric matcher is covered under a classified Privacy Impact Assessment approved by DOJ August 28, 2018.

System Of Record Notices (SORN): The MXU system is covered under Systems of Records Notices Justice/FBI-002, FBI Central Records System[57] and Justice/FBI-022, FBI Data Warehouse System.[58]

Data Elements Received by War Crimes Hunter:

Information that the FBI may share with HRVWCU varies widely depending on the dataset gallery the facial image matched. For example, MXU may only be able to provide a link to the original photo or device to which the match was made and the associated FBI case. In other scenarios where MXU galleries are more robust, biographic information or links to other identity repositories may be provided.

Due to classification levels, any information shared back to HRVWCU will be done offline, by IHRU, through appropriate, secure channels.

[56] For more information *see* https://www.nsa.gov/news-features/declassified-documents/ukusa/.
[57] 63 FR 8659, 8671 (February 20, 1998).
[58] 77 FR 40630 (July 10, 2012).

Retention by Partner and Permissible Uses:

MXU will retain the WCH data in its sensitive biometric matcher under handling and notification restrictions identified by the data owner (DHS). MXU will use WCH data to identify possible human rights violators in seized media or biometrically-enabled FBI case data that is routed to MXU's sensitive biometric identification system. MXU maintains a program level data retention Standard Operating Procedures (SOP) which dictates that the unit review each data set annually for relevancy, justification and currency.

As WCH does not include any other PII with WCH images (besides suspected grounds of inadmissibility), any potential match made against WCH images in MXU will only alert an MXU user to contact HRVWCU for a follow up. A potential match of a user's submission to WCH images will not, by itself, lead to an arrest, detention, or the denial of benefits.

Onward Transfer:

Authorized FBI, state, local, federal law enforcement, and intelligence agency users may query probe photos against the MXU face database where unidentified WCH images will be held. MXU returns likely matches after adjudication by MXU's facial examiners.

WCH images may be shared with federal agencies, state, local, tribal, and territorial law enforcement agencies, intelligence partners, and foreign and international agencies for national security, law enforcement, criminal justice, intelligence, and national defense purposes. This sharing will be consistent with the restrictions and routine uses outlined in the DHS/ICE-009 External Investigations SORN.[59] Potential matches to WCH images by MXU users will only result in an alert to the user to contact HRVWCU, through IHRU, for a follow up.

Correction and Redress:

The Attorney General has exempted this system of records from the notification, access, and contest procedures of the Privacy Act. If records access would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the FBI in its sole discretion. All requests for access should follow the guidance provided on the FBI's website.[60] Individuals may mail, fax, or email a request, clearly marked ''Privacy Act Request,'' to the following address:

Federal Bureau of Investigation
Attn: FOI/PA Request, Record/Information Dissemination Section
170 Marcel Drive, Winchester, VA 22602–4843

[59] DHS/ICE-009 External Investigations, (85 FR 74362) November 20, 2020.
[60] http://foia.fbi.gov/ requesting_records.html.

Requests may be faxed to 540–868–4995/6/7 or a scanned copy can be emailed to: foiparequest@ic.fbi.gov. The request should include a general description of the records sought and must include either a completed Department of Justice Certification of Identity Form (DOJ–361),[61] or a letter that has been notarized which includes: The requester's full name, current and complete address, and place and date of birth or be submitted under penalty of perjury of law pursuant to 28 U.S.C. 1746.

In the initial request the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request.

Individuals desiring to contest or amend information maintained in the system should direct their requests according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. The envelope and letter should be clearly marked ''Privacy Act Amendment Request'' and comply with 28 CFR 16.46 (Request for Amendment or Correction of Records). Some information may be exempt from contesting record procedures as described in the section entitled ''Exemptions Claimed for the System.'' An individual who is the subject of a record in this system may amend those records that are not exempt.

[61] *Id.*