Privacy Impact Assessment

for

Immigration and Customs Enforcement Operational Use of Publicly Available Information Including Social Media Information for Law Enforcement Investigations

DHS Reference No. DHS/ICE/PIA-064

December 15, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) has a statutory mission to enforce the nation's immigration laws and combat transnational crime. To achieve its mission, ICE personnel collect information from a variety of sources, including publicly available information on the internet and on social media platforms. ICE personnel use publicly available information found on the internet, including on social media platforms, in support of ICE's law enforcement mission. ICE is conducting this Privacy Impact Assessment (PIA) because some of the publicly available information that its personnel collect, maintain, or share may include personally identifiable information (PII).[1] This Privacy Impact Assessment focuses on the collection and use of publicly available information including social media information for law enforcement investigations, leaving in-depth analysis of maintenance and sharing to the respective Privacy Impact Assessments for ICE systems in which the data is ultimately stored. These systems are listed in the Appendix to this Privacy Impact Assessment.

Introduction

To fulfill its statutory mission, ICE uses a variety of sources from which it collects information related to criminal investigations and immigration enforcement matters. Accordingly, ICE may access, collect, and use information available on the internet and social media platforms,[2] including publicly available information as one of its information assets.[3] ICE maintains compliance with DHS Directive 110-01, *Privacy Policy for Operational Use of Social Media*,[4] and

[1] DHS defines "personally identifiable information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or employee of or contractor to the Department. *See* DHS INSTRUCTION MANUAL 047-01-007, REVISION 3 (2017), HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII), *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[2] DHS defines "social media" as the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media takes many different forms, including but not limited to, web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. The definition of "social media" does not include internal Department intranets or applications. *See* DHS LEXICON, REVISION 2 (2017), *available at* https://www.dhs.gov/publication/dhs-lexicon.

[3] DHS defines "publicly available information" as "unclassified information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." "Open source" information is a form of publicly available information and defined as "unclassified information that has been published or broadcast in some manner to the general public, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." *See* DHS LEXICON, REVISION 2 (2017), *available at* https://www.dhs.gov/publication/dhs-lexicon.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY DIRECTIVE 110-01, OPERATIONAL USE OF SOCIAL MEDIA (2012), *available at* https://www.dhs.gov/privacy-policy-guidance.

its accompanying Instruction, 110-01-001.[5] These policy documents establish privacy policy and requirements for DHS and its components for the access, collection, use, maintenance, retention, disclosure, deletion, and destruction of personally identifiable information in relation to the operational use of social media. Due to the trend toward including interactive, social media-style features on "traditional" internet sites, ICE has determined DHS's Privacy Policy governs the collection of personally identifiable information online on all internet sites,[6] not only on social media platforms.

ICE may only access information online from open source sites (e.g., blogs, news sites, public record repositories) and on social media platforms that is publicly available.[7] This includes any public messages, posts, and media (e.g., photos, documents, geolocation information).[8] The ICE offices that access publicly available social media information as part of their law enforcement activities include the following:

- Office of Homeland Security Investigations (HSI): HSI is the primary investigative arm of DHS and combats criminal organizations exploiting U.S. trade, travel, financial, and immigration systems.
- Office of Professional Responsibility: The Office of Professional Responsibility is responsible for upholding ICE's professional standards through a multi-disciplinary approach of security, inspections, and investigations. The Office accomplishes its mission by investigating allegations of employee misconduct; conducting independent reviews and audits of ICE programs, offices, and detention facilities; measuring compliance with applicable policies, regulations, and laws; and administering ICE's internal security program to protect and secure people, information, and facilities.[9]

This Privacy Impact Assessment covers the following items related to ICE employee and contractor use of publicly available and social media information in law enforcement investigations:

- ICE's operational uses of publicly available online content and social media information;
- ICE's use of technology and tools that collect and analyze publicly available information including social media information;

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY INSTRUCTION 110-01-001, OPERATIONAL USE OF SOCIAL MEDIA (2012), *available at* https://www.dhs.gov/privacy-policy-guidance.
[6] This Privacy Impact Assessment only assesses ICE's collection and use of publicly available information including social media information for law enforcement investigations. This Privacy Impact Assessment does not cover ICE undercover operations, which are governed by separate legal and privacy guidelines.
[7] *Id*.
[8] Geographic data may come from publicly shared social media information.
[9] This Privacy Impact Assessment does not address use of publicly available and social media information by ICE Office of Professional Responsibility in support of its internal security program to protect and secure people, information, and facilities.

- ICE's use of the deep and dark webs;
- ICE's policy and Rules of Behavior (ROB) for ICE personnel use of social media information;
- First Amendment and Equal Protection restrictions placed on ICE online collections;
- Select mitigation measures for the use of tools to access, collect, and/or analyze publicly available information, including social media information; and
- identification of privacy risks and steps that ICE takes to mitigate risks to personally identifiable information.

ICE's Operational Uses of Publicly Available Information, including Social Media Information

This section details how each ICE program engages with social media and how publicly available information obtained from social media or other publicly available online content is used in furtherance of ICE's law enforcement mission.

HSI Use of Publicly Available Online Content and Social Media Information

ICE HSI investigations cover a broad range of topics, including, but not limited to, national security threats, financial and smuggling violations (including illegal arms exports), financial crimes, commercial fraud, human trafficking, narcotics smuggling, child sexual abuse/exploitation, and immigration fraud. Given HSI's vast portfolio, its agents and support personnel rely on a variety of sources of information to generate leads, including information from publicly available sources and social media. Generally, HSI searches of publicly available information will have a nexus to an existing investigation; however, if the information or social media posting is indicative of a criminal violation enforceable by ICE HSI (e.g., child sexual abuse material, an online marketplace for narcotics), that information can be used to initiate an investigation. The following examples provide a comprehensive list of the ways in which HSI personnel use publicly available content and social media information. In the future, if HSI's use of such information deviates from the list below, this Privacy Impact Assessment will be updated to provide additional transparency on the new uses as well as assess any potential privacy risks and appropriate mitigation measures.

HSI uses social media and publicly available information for tactical planning activities prior to a specific law enforcement action to ensure safety of officers and other individuals at or near the scene. Any information that HSI uses in this context is documented in the Investigative Case Management system (ICM) and in the Repository for Analytics in a Virtualized Environment (RAVEn).[10] HSI also uses publicly available information, including social media

[10] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact

information, to enhance information from various government and law enforcement databases in furtherance of its law enforcement investigations.[11]

Social media searches are conducted as needed and must be associated with a specific case, operation, or mission-related purpose, such as combatting human trafficking or money laundering.

HSI may consolidate corroborated open source and social media information with information maintained in government databases and create a report that is entered into an ICE case management or lead generation system.[12] The information may then be shared within HSI for investigative action.

HSI may also conduct open source and social media research on schools as part of the certification[13] and recertification[14] compliance process of the Student Exchange and Visitor Program (SEVP).[15] For example, HSI may use publicly available information to verify a school's petition as part of the Student Exchange and Visitor Program certification, recertification, or unannounced review (e.g., following up on tips received from federal agents or the Field Representative Units). HSI does not target[16] individuals, such as school officials or students, when researching schools to determine the institutions' compliance with SEVP certification requirements.

HSI personnel also will access and use publicly available information online to verify data contained on a school's Form I-17, "Petition for Approval of School for Attendance by Nonimmigrant Student."[17] HSI will use online content, including social media information, to verify the accuracy of the school's official name and other data listed on the Form I-17, such as

---

Assessment for the Investigative Case Management System (ICM), *available at* https://www.dhs.gov/privacy-documents-ice. Any information introduced as evidence in a prosecution would be obtained directly from the social media platform via subpoena or search warrant. *See also* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Repository for Analytics in a Virtualized Environment (RAVEn), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR LEADTRAC, DHS/ICE/PIA-044, and INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), DHS/ICE/PIA-045, *available at* www.dhs/gov/privacy-documents-ice.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR LEADTRAC, DHS/ICE/PIA-044, and INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), DHS/ICE/PIA-045, *available at* www.dhs/gov/privacy-documents-ice.

[13] The Student and Exchange Visitor Program's (SEVP) School Certification Unit certifies schools to accept F (academic) and M (vocational) visa holder students.

[14] Designated School Officials, acting on behalf of SEVP-certified institutions, must complete recertification every two years to confirm compliance with SEVP eligibility, record keeping, and recording requirements on F and/or M visa holder students at various types of schools.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE AND VISITOR PROGRAM (SEVP), DHS/ICE/PIA-001, *available at* www.dhs/gov/privacy-documents-ice.

[16] ICE SEVP does not target individuals outside of HSI's regulatory requirements to vet and conduct routine background checks on school officials/students and refer potential visa violators for further investigation.

[17] Form I-17, Petition for Approval of School for Attendance by Nonimmigrant Student, *available at* https://studyinthestates.dhs.gov/sevis-help-hub/school-records/school-certification/form-i-17-initial-certification.

the school's county, city, state, and address.

HSI may also review the school's social media homepage and school website to verify information on the Form I-17, including program(s) of instruction information (e.g., listed courses, course descriptions, schedules, graduate requirements). If HSI finds discrepancies between the information posted on the Form I-17 and what is publicly available, HSI will generate a lead to the field for further investigation.

Additionally, HSI may use publicly available information to investigate F-1 and M-1 student visa holders who are suspected of overstaying their visas or otherwise violating the terms of their admission into the United States.[18]

Further, HSI uses publicly available information, including social media information to investigate suspected illegal activity by foreign students on college campuses,[19] or other administrative issues related to a foreign student's non-immigrant status. As described above, any HSI use of social media information must have a nexus to an authorized investigation or the social media information itself be indicative of a crime enforceable by ICE HSI.

All information HSI retrieves from social media will be documented in the appropriate ICE case management or lead generation system.[20]

HSI also assists the Department of State in conducting the initial vetting of visa applicants.

ICE Office of Professional Responsibility Use of Publicly Available Online Content and Social Media Information

The ICE Office of Professional Responsibility will complement its investigations of allegations of criminal violations or misconduct by ICE personnel with publicly available information. ICE Office of Professional Responsibility will review publicly available postings on the social media accounts associated with ICE employees under investigation to further investigate any claims of criminal or administrative misconduct submitted to the Office by the public or other ICE employees. ICE Office of Professional Responsibility collects any information relevant to the investigation, documenting it in the Office's case management system, the Joint Integrity Case

[18] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for LeadTrac, DHS/ICE/PIA-044, and U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for Student and Exchange Visitor Program (SEVP), DHS/ICE/PIA-001, a*vailable at* www.dhs/gov/privacy-documents-ice.

[19] For example, foreign students suspected of stealing intellectual property to provide to their home countries.

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), *available at* https://www.dhs.gov/privacy-documents-ice. Any information introduced as evidence in a prosecution would be obtained directly from the social media platform via subpoena or search warrant. *See also* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEn), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

Management System (JICMS).[21]

ICE Use of Technology and Tools that Collect and Analyze Publicly Available Information Including Social Media Information

ICE uses commercial databases and analytical products to help search, monitor, and process publicly available data from online, public records data sources, and social media platforms pursuant to ongoing investigations. ICE offices and programs may use one or a combination of tools to accomplish their mission. Prior to its use of any technology or tool that accesses, collects, and/or uses personally identifiable information, an ICE program must submit a Privacy Threshold Analysis (PTA) to ICE Privacy to assess the technology or tool's impacts on individual privacy. All Privacy Threshold Analyses must be submitted to and approved by the DHS Privacy Office. All personnel who use a technology or tool must be trained on the appropriate uses of that instrument. The following is a description of the tools that ICE uses to achieve its statutory mission using publicly available information. Each tool may raise unique privacy risks, which are assessed using the Fair Information Practice Principles as discussed later in this Privacy Impact Assessment.

Analytical Search Engines and Data Aggregators

ICE also uses tools that collect and compile information from multiple publicly available sources across the internet in support of open law enforcement investigations. These aggregator tools retrieve data from credit bureaus, government public records, news sites, and other publicly available information resources. The data the aggregator retrieves is available to the public, either through internet searches or purchase. Data aggregators present data from search queries in a format that is meaningful or useful to the user. Data aggregators used by ICE are specifically designed to search public records and publicly available social media information, filter duplicate information, and present returned information in a manner that is useful to ICE personnel and directly related to an ICE investigation.[22]

ICE users will access data aggregator tools via a web portal and enter the search terms directly related to a person of interest (e.g., fugitive, suspect).[23]

Link Analysis Applications

Link analysis applications capture digital connections. ICE may use link analysis

[21] The Joint Integrity Case Management System (JICMS) is owned by U.S. Customs and Border Protection and is used by ICE. For more information, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044, *available at* www.dhs.gov/privacy-documents-cbp.

[22] ICE is prohibited from using data aggregators or other tools to access, collect, or use data that ICE is otherwise prohibited from accessing, collecting, or using.

[23] Persons Of Interest (POI) may include individuals who are reasonably suspected of a crime, are the subject of investigative interest based on the individuals' association with illegal cross-border activity or another criminal network, such as terrorist groups, are wanted in connection with a crime (e.g., arrest warrant), or for whom there is investigative evidence linking the individual to criminal acts within ICE's mission to enforce (e.g., bombing).

applications in support of open investigations. These applications aggregate connected online accounts and social media data to assist investigators with identifying possible connections to an investigation. This is also known as "link analysis." Link analysis helps investigators identify and assess suspected criminal networks by detecting similarities.[24]

The data must be reviewed by an ICE investigator, who is required to assess the information and corroborate it before it can be used in an investigation.

Automated Collection Tools

ICE may use automated applications or tools that collect information from publicly available websites and chatrooms identified as relevant to ICE investigations. This process, sometimes referred to as "scraping" is an automated process that copies and collects website data that has been pre-designated by a user as related to an investigation, on a recurrent basis, then loads the copied data into a database for later analysis and use.

ICE personnel will use all available and relevant information such as witness statements, investigative reports, and other documentary evidence, to assess the accuracy and authenticity. ICE is not permitted to collect entire websites or information unrelated to an investigation. The site selection must be submitted to an ICE supervisor for approval before it can be subject to an automated collection tool.

The ICE supervisor must verify that the website or chatroom contains relevant and credible evidence of suspected violations within ICE's statutory law enforcement mission and that the parameters of collection are narrowly tailored to collect only that information directly relevant to a law enforcement investigation. As noted, collection and analysis is only permitted on subjects and information determined to be relevant to and within the scope of an investigation.

Automated collection tools do not modify data in any way. All collection by the tool is passive. These tools do not violate or circumvent privacy settings and protections placed on the information by a website or chatroom. These tools do not "friend" or "follow" social media accounts, may not post content on social media websites, and may not prompt the collection of information from other individuals or accounts. All collections are manually reviewed by ICE personnel for credibility and relevance to the open investigation. If data collected by these tools is deemed irrelevant, then ICE deletes the information, and it will not be stored or retained in the repository. Any information retained by ICE will be documented in the relevant case file, including the tools that were used to acquire the information and the source of the information. If at any point a site is determined to no longer be relevant to the ICE investigation for which its use was initiated,

[24] Link analysis tools also can sort, match, and link multiple open-source databases. The link analysis tool user interface platforms can provide further attribution to the subject of an authorized, ongoing investigation. HSI will use link analysis tools to identify the following information directly related to an open investigation: criminal suspects, witnesses, the location of at-large individuals, businesses, and assets of targets of investigations for potential arrest, seizure, and forfeiture. HSI can access link analysis tools through a web-based portal (username/password) and/or submit queries directly to the tools via Short Messaging Service (SMS) text.

the collection will be immediately discontinued. Similarly, if ICE becomes aware that a site may no longer present credible information, then automated collections will be discontinued immediately.

Recurrent Query Platforms/Tools

ICE uses web-based platforms/tools to recurrently query open source websites and publicly available social media accounts for information directly related to ICE investigations. A platform must only retrieve information that would be accessible to the public through basic internet searches (e.g., a web browser search); therefore, recurrent query platforms/tools may not be used to access information that requires an account (e.g., a social media profile). ICE uses the information gathered through use of the platforms/tools to generate investigative leads. Prior to the procurement or development of a query platform/tool, ICE Privacy, through the Privacy Threshold Analysis process, will confirm that the platform/tool does not violate any website or social media account's privacy settings on which the tool is intended to be used.

ICE personnel must review responsive information to determine whether it is accurate/corroborated and whether the information is relevant to an investigation. Users can select relevant information in the results that will then automatically be added to a report that can be exported from the web portal for later ingestion into an ICE system. Information not selected (because it is determined not to be relevant to the specific investigation) will be deleted from the portal by the vendor. By selecting information as relevant to an investigation, the platform search algorithms are enhanced for future searches. If a report is exported, the ICE user will re-initiate checks against government systems and again manually search for additional open source information for corroboration prior to entering information into any ICE system or generating a lead.

ICE Policy for Using Publicly Available Online Content and Social Media Information

In 2012, the then-ICE Director issued a memorandum to all ICE personnel titled "Use of Public and Non-Public Online Information"[25] outlining core principles for ICE law enforcement use of online information (hereinafter "Morton Memo"). The memorandum laid out key principles under which ICE personnel are allowed to use social media for operational purposes. ICE use of publicly available information for operational purposes must abide by the 2012 Morton Memo and DHS Privacy Policy 110-01. Key principles of the 2012 Morton Memo include the following:

- Obtaining Information from Unrestricted Sources: Law enforcement personnel may obtain information from publicly accessible online sources and facilities under the same conditions as those by which they may obtain information from other sources generally

[25] U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, POLICY GUIDANCE MEMORANDUM 100821.1 USE OF PUBLIC AND NON-PUBLIC ONLINE INFORMATION (2012), on file with ICE Privacy. This memorandum is also referred to as the "2012 Morton Memo." This memorandum is being reviewed and may be updated or superseded as needed.

open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.

- Obtaining Identifying Information about Users or Networks: Law enforcement personnel may use available software tools in their intended lawful manner under the same circumstances in which ICE guidelines and procedures permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, law enforcement personnel may not use software tools, including those which are generally available as standard operating system software, to circumvent restrictions placed on system users.
- Real-Time Communications: Law enforcement personnel may passively[26] observe and log real-time electronic communications open to the public under the same circumstances in which they may attend a public meeting.
- Accessing Restricted Sources: Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into a private space.
- Online Communications Generally: Law enforcement personnel may use online services to communicate in the same manner as they may use other types of communication tools, such as the telephone and the mail. Law enforcement personnel should retain the contents of a stored electronic message if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

Any update to these principles will necessitate a corresponding update to this Privacy Impact Assessment.

Additionally, ICE Privacy works with relevant ICE program offices to ensure that ICE guidance and policy remains current and consistent with the evolution of internet use in law enforcement operations. As new publicly available information programs or tools are used, procured, or developed by ICE, ICE Privacy may require more focused and tailored rules of behavior and other safeguards for ICE's uses of publicly available information. Rules of behavior are reviewed for compliance with DHS and ICE policy, including the 2012 Morton Memo. ICE Privacy, ICE Office of the Principle Legal Advisor, and the DHS Privacy Office must approve new and updated ICE rules of behavior.

First Amendment and Equal Protection restrictions

[26] As discussed in this Privacy Impact Assessment, passive observation includes a prohibition on communicating directly with an individual, eliciting websites to collect information, responding to an individual's posts, or posting content meant to elicit a response from an individual.

In 2019, the then-DHS Secretary reaffirmed that DHS personnel would observe and protect individuals' First Amendment rights, regardless of the medium through which those rights are exercised.[27] ICE, as a Component of DHS, will not collect information regarding an individual's religious beliefs; political and personal beliefs; lawful associations; or protest unless, consistent with the Privacy Act, the information is pertinent to and within the scope of an authorized criminal, civil, or administrative law enforcement activity (e.g., a crime within the scope of ICE law enforcement authorities). ICE use of social media information is directly related to an open investigation and often subject-focused, meaning that searches and collections are centered around targets of investigation or information that is, on its face, relevant to an open criminal, civil, or administrative investigation undertaken pursuant to ICE law enforcement authority (e.g., child sexual abuse material).

In addition, the Privacy Act of 1974[28] generally prohibits ICE from collecting records describing how an individual, defined as a U.S. citizen or Lawful Permanent Resident, 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," or if either a law or the individual about whom the record is maintained expressly authorizes such maintenance.[29] ICE personnel must successfully complete social media training, created by ICE Privacy in consultation with the ICE Office of the Principle Legal Advisor and the DHS Office for Civil Rights and Civil Liberties, on how to identify First Amendment activity, ensure there is a lawful basis to collect the information, and confirm the collection will be performed using the least intrusive means[30] possible to accomplish the authorized law enforcement action or activity.

DHS also prohibits the consideration of protected individual characteristics (i.e., race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, and disability) in investigation, screening, and law enforcement activities in all but the most exceptional instances. The Department of Justice "Guidance For Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, Gender Identity, and Disability" (DOJ Guidance)[31] is the policy of DHS as it applies to federal law enforcement

[27] *See* SECRETARY OF HOMELAND SECURITY MEMORANDUM, INFORMATION REGARDING FIRST AMENDMENT PROTECTED ACTIVITIES (2019), *available at* https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.
[28] 5 U.S.C. § 552a.
[29] 5 U.S.C. § 552a(e)7.
[30] "Least-Intrusive-Means" doctrine refers to the requirement that ICE begin with a collection method that is less invasive for the individual, and only increasingly so if no other less invasive collection methods exist. For example, ICE requires its investigators to use information available via public internet searches.
[31] *See* U.S. Department of Homeland Security Policy Guidance Memorandum: Guidelines for Enforcement Actions In Or Near Protected Areas (2021); The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities (2013), *available at* 21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf (dhs.gov). *See also* U.S. DEPARTMENT OF JUSTICE, GUIDANCE FOR FEDERAL LAW ENFORCEMENT AGENCIES REGARDING THE USE OF RACE, ETHNICITY, GENDER, NATIONAL ORIGIN, RELIGION,

personnel and federal non-law enforcement personnel engaged in or supporting federal law enforcement activity and intelligence activity conducted by Federal law enforcement agencies.[32] Consideration of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, and disability in DHS law enforcement activities occurs only in strict accordance with DOJ Guidance.[33]

DHS personnel may use protected individual characteristics only when a compelling governmental interest is present, and only in a manner narrowly tailored to meet the compelling interest. The Department of Justice Guidance does not apply to (1) interdiction activities at the border or its functional equivalent (such as airports, seaports, and other ports of entry) and related traveler and cargo vetting activities, as well as protective and inspection activities; (2) non-law enforcement screening activities; and (3) all activities that use country of birth or nationality as a security screening, enforcement, or investigative criterion.[34] These activities remain subject to Department of Homeland Security's 2013 policy.[35]

Further, information collection supporting HSI administrative immigration enforcement activities is governed by the DHS policy "Guidelines for Enforcement Actions in or Near Protected Areas," that superseded previous ICE policy.[36] The policy discourages actions that may detrimentally affect the willingness of an individual to seek essential services, including the monitoring of social media accounts associated with protected areas. Protected areas include churches, schools, and healthcare facilities. The policy specifically constrains "immigration enforcement surveillance" at these locations. ICE personnel are required by policy to conduct enforcement actions and information gathering activities in support of an enforcement action, in such a manner as to avoid targeting these protected areas.[37]

Select Mitigation Measures for the Use of Tools to Access, Collect, and/or Analyze Publicly

---

SEXUAL ORIENTATION, GENDER IDENTITY AND DISABILITY (May 25, 2023), *available at* https://www.dhs.gov/publication/guidance-federal-law-enforcement-agencies-regarding-use-race-ethnicity-gender-national.

[32] *See* U.S. Department of Homeland Security Policy Statement 500-02 Reaffirming the Commitment to Nondiscrimination in Department of Homeland Security Activities (May 25, 2023), *available at* https://www.dhs.gov/publication/department-homeland-security-commitment-nondiscriminatory-law-enforcement-and-screening.

[33] *Id.*

[34] *Id.*

[35] *See* U.S. Department of Homeland Security Memorandum For Component Heads, the Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities (April 26, 2013), *available at* https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0_1.pdf

[36] *See* U.S. DEPARTMENT OF HOMELAND SECURITY POLICY GUIDANCE MEMORANDUM: GUIDELINES FOR ENFORCEMENT ACTIONS IN OR NEAR PROTECTED AREAS (2021), *available at* https://www.dhs.gov/sites/default/files/publications/21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf.

[37] *See* U.S. HOMELAND SECURITY POLICY MEMORANDUM: GUIDELINES FOR ENFORCEMENT ACTIONS IN OR NEAR PROTECTED AREAS (2021), *available at* https://www.dhs.gov/sites/default/files/publications/21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf.

Available Information, Including Social Media Information

The following are additional safeguards applicable to the use of tools, known at the time of this Privacy Impact Assessment, to facilitate ICE's use of publicly available and social media information. If ICE proposes to use additional services/platforms/tools/applications in the future, it will complete required Privacy Threshold Analyses and update this Privacy Impact Assessment as appropriate.

Use of Application Programming Interfaces/"Scraping"

The use of application programming interfaces (APIs) and/or scraping can be inconsistent with a website or social media platform's terms of service. Therefore, ICE's use of tools/applications that facilitate their use could impact personal privacy. Accordingly, some mitigation measures are in place, as discussed above, for the use of these tools/applications.

The use of APIs that facilitate scraping is akin to the use of automated collection tools. Therefore, the use of scraping tools/applications must satisfy the requirements for use of automated collection tools as discussed above.

For example, users must first assess the accuracy and authenticity of the information sought for collection and then receive supervisory approval to use this tool/application. The supervisor must verify that the site or platform targeted for collection contains relevant and credible information of suspected violations related to an open investigation and that the parameters of collection only collect information directly relevant to the investigation.

ICE is not permitted to collect entire websites or information unrelated to the investigation. Further, use of these tools/applications will be in a manner that respects all privacy settings. And, if at any point a site or platform is determined to no longer be relevant to the ICE investigation for which its use was initiated, or it may no longer present credible information, the collection by the tool/application will be immediately discontinued.

Network Analysis

Network analysis tools/applications are the same as link analysis applications discussed above. Therefore, use of these tools/applications will be in a manner consistent with the parameters outlined above. Additionally, there is a privacy risk associated with analyzing a person's network, including that the individuals who are a part of that network may have no connection to the suspected individual and/or illegal activity. For example, simply liking a post, tagging or being included in a photo, or having a relationship with a suspected individual does not indicate a connection to criminal activity under investigation. To mitigate this risk, establishing parameters around perceived relationships is critical, such as limiting collection on the number of connections out from the suspected individual (i.e., "hops") and ensuring a direct connection to the person under investigation and criminal activity by the connected individual.

Supervisors will review and confirm the user's written justification. Also, supervisors will verify ICE personnel compliance with agency-wide and tool-specific training and adherence to the applicable rules of behavior. Supervisors may require additional safeguards if they identify inconsistencies or other concerns.

Keyword Queries:

Use of keyword queries by a tool/application is the same as use of recurrent query platforms/tools discussed above. Therefore, use of keyword queries in tools/applications will be in a manner consistent with the parameters outlined previously. For example, information sought through keyword queries must be directly related to an ICE investigation. Only information accessible to the public through basic internet searches can be retrieved; therefore, the keyword queries tool/application cannot be used to access information that requires an account (e.g., social media profile). Users must review responsive information to assess its accuracy and direct relevance to an open investigation. Further, users must corroborate the information before it may be used. If information is retrieved that is not directly relevant to an open investigation, then it must be deleted and the collection discontinued.

Additionally, there is a risk that using certain keywords to search an individual's publicly available information may implicate the "purpose specification" principle. Accordingly, any keywords used to query publicly available information will be designed in such a way as to not profile, target, or discriminate against any individual for lawfully exercising their First Amendment rights. Keywords will be directly relevant to the suspected criminal actions of the person of interest, specific events, or specific locations directly related to the investigation. To ensure that keyword searches are conducted in an authorized manner, keywords used to query publicly available information will be documented and subject to periodic review by the Office of the General Counsel, ICE Privacy, DHS Privacy, and the DHS Office for Civil Rights and Civil Liberties. Additionally, ICE Privacy will meet monthly with the program to assess how keywords are being used.

Vendor Limitations

There is a risk that ICE's use of vendors or contractors could implicate the "purpose specification" principle. As noted previously, ICE may not use a vendor-provided tool or application, nor may a contractor perform work on behalf of ICE, in a manner inconsistent with governing law and policy. Contractors and vendors should not collect, use, maintain, or disseminate personally identifiable information that ICE does not have the authority to collect, use, maintain, or disseminate. For example, while contractors may collect personally identifiable information related to First Amendment protected activity when operating independent of any government involvement, contractors may not collect such personally identifiable information to fulfill any obligations to the government.

Additionally, there is a risk that a vendor could have access to personally identifiable information ICE users input into the tools/applications and ICE sensitive law enforcement activities. Accordingly, while vendors will retain administrative functions within a tool/application, ICE will maintain control of all use restriction and auditing capabilities, unless any additional functions assigned to the vendor are detailed in the contract or agreement and are performed under general ICE direction. Additionally, the vendor may not use personally identifiable information input into the tool/application by an ICE user to further refine and/or train the tool or its model(s).

Other tools/applications

The platforms or tools that ICE uses on publicly available information, including social media information, for investigations may include other applications or functions that are not permitted for use at this time. For example, ICE may not use emotional or sentiment analysis tools/applications, "risk profile," facial recognition, or reverse image searching tools in this context. If in the future ICE wishes to reevaluate the tools it uses in this context, it will coordinate with the DHS Privacy Office and the Office for Civil Rights and Civil Liberties to assess the proposed tool's efficacy and assess any related potential privacy, civil rights, and civil liberties risks.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[38] articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974. [39]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. [40] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222.[41] Because ICE use of publicly available and social media information is not

[38] 5 U.S.C. § 552a.
[39] 6 U.S.C. § 142(a)(2).
[40] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[41] 6 U.S.C. § 142.

an information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the potential privacy impact of ICE use of publicly available and social media information.

1. Principle of Transparency

Notice of ICE operational use of publicly available information including social media information for law enforcement investigations is provided by the publication of this Privacy Impact Assessment and relevant system of records notices governing systems in which social media information collections are maintained.[42] ICE also includes notice of other instances of its use and maintenance of publicly available information including social media information in an ICE system via that system's Privacy Impact Assessment.[43] Since ICE collection and use of publicly available and social media information collections are law enforcement activities related to law enforcement investigations, it may not be feasible to provide direct notice to individuals at the time their information is collected from publicly available sources because to do so could provide notice of sensitive, ongoing law enforcement investigations.

Privacy Risk: There is a risk that individuals who use publicly available platforms, including social media platforms, may not know that the information they publicly share on the platform may be collected by ICE to support an open law enforcement investigation.

Mitigation: The risk is partially mitigated. To the extent information in this Privacy Impact Assessment is made publicly available, this Privacy Impact Assessment provides notice of ICE's collection, use, and maintenance of publicly available information, including social media information, to support law enforcement investigations.

While publicly available sources, including social media platforms, may provide notice of the potential use of information posted to the sites for law enforcement investigations pursuant to lawful process, notice of ICE's use of publicly available information as discussed in this Privacy Impact Assessment often is not provided by the platform. Further, as noted previously, ICE cannot notify an individual when their information is collected by ICE from publicly available sources because doing so could risk informing a target of an active law enforcement activity of an open investigation.

To mitigate this risk, ICE personnel may only view information that is available to the public (e.g., not behind added privacy walls). ICE assumes the individual is on notice that their information, not subject to additional privacy restrictions, is viewable by anyone that has access to the publicly available source/social media platform. In other words, ICE will only access publicly available sources to collect and analyze data that is available (either for free or for

[42] For a list of all ICE system Privacy Impact Assessments, *see* www.dhs.gov/privacy-documents-ice. For a list of Systems of Records Notices published by ICE, *see* https://www.dhs.gov/system-records-notices-sorns.
[43] *See* the Appendix to this Privacy Impact Assessment for a list of ICE systems that contain publicly available and social media information.

purchase) to the public and directly relevant to an open law enforcement investigation.

Privacy Risk: There is a risk that a third party may post an individual's information to a website or social media platform without the individual's consent and that information is then used by ICE in a law enforcement investigation.

Mitigation: This risk cannot be mitigated. At the time of collection, ICE cannot determine whether an individual provided a third party with consent to publicly post their information to a website or social media platform. Similarly, ICE cannot determine whether an individual understands the privacy policies and settings of a social media platform before they posted the information to a publicly available source.

Privacy Risk: There is a risk that individuals will not know that their information was obtained by ICE to support an open law enforcement investigation.

Mitigation: This risk is partially mitigated.

Targets of investigations and their associates who are directly related to the law enforcement matter being investigated may not be aware ICE is actively collecting their information from publicly available sources/social media platforms. Providing notice to these individuals could inform them that they are the target of an actual or potential law enforcement activity or reveal ICE's investigative interest in them.

All individuals present in the United States, however, have constitutional protections in criminal proceedings entitling them to discovery production.[44] The discovery obligations of federal criminal prosecutors established by the Federal Rules of Criminal Procedure include Rule 16, and Rule 26.2. Additionally, the requirements of 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*,[45] and *Giglio v. United States* apply.[46] In court, each party is responsible for producing evidence upon which it seeks to rely in the litigation. Therefore, if ICE seeks to use publicly available information or evidence derived from such information to sustain any charge or otherwise use as evidence, it would be required to produce that information to the defendant.

Further, as noted previously, ICE may not collect information that is not directly relevant to an open law enforcement investigation, which helps mitigate the number of individuals potentially impacted by ICE's use of publicly available information to support law enforcement investigations.

2. Principle of Individual Participation

As with notice, ICE cannot involve the individual in the process of using their personally

[44] Discovery is the pre-trial process parties use to gather information in preparation for trial. Parties may obtain discovery regarding any nonprivileged matter in the form of records, testimony, and other information, that is relevant to any party's claim or defense. *See* Fed. R. Civ. P. 26-37, and Fed. R. Crim. P. 16 and 26.2, *available at* https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.
[45] 373 U.S. 83 (1963).
[46] 405 U.S. 150 (1972).

identifiable information to support open investigations. To seek consent for the collection, use, dissemination, and maintenance of their personally identifiable information could risk exposing an ongoing law enforcement investigation. To mitigate this risk, ICE is not permitted to access and use information from publicly available sources that is subject to additional privacy safeguards. For instance, social media platforms may allow individual users to set privacy restrictions on who may access and see their content. If these restrictions are in place, ICE may not access that information. Additionally, individuals may edit, correct, or update information shared in their own posts or in comments they made to the posts of others.

An individual's ability to access or amend information in ICE law enforcement information systems is limited by law and policy due to the need to protect the integrity of national security or law enforcement sensitive information.[47] Access to ICE records might also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, harm victims, or avoid detection or apprehension. Individuals may submit requests for information access and correction as permitted by the Privacy Act, and the requests will be reviewed on a case-by case basis. Individuals seeking to correct records, or seeking to contest their content, may submit a request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement Office of Information Governance and Privacy
Attn: Privacy Unit
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

Privacy Risk: There is a risk that individuals cannot access and amend inaccuracies in ICE systems that maintain publicly available information, including social media information.

Mitigation: The risk is partially mitigated. For example, vendors of commercial data should endeavor to ensure their information collections contain near real-time data for the efficacy of the product that ICE would utilize. However, if a vendor collects data from publicly available sources, any edit, correction, or update the individual makes to the information in the data sources might be delayed before it is reflected in the vendor database. Moreover, vendors may not notify ICE when an edit, update, or correction occurs within its own proprietary database. Likewise, information ICE accesses from other publicly available sources, including social media information, may be amended without notice to ICE.

In accordance with ICE policy, ICE users will research and corroborate the source data to ensure that the information is as accurate, timely, and complete prior to using the data to generate an investigative lead or pursuing a law enforcement action. Likewise, as noted above, users will

[47] *See* DHS/ICE-009 External Investigations, 85 FR 74362, (November 20, 2020), Final Rule for Privacy Act Exemptions, 74 FR 4508 (August 31, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

document the source(s) of information, including whether a vendor was used to obtain the information, in the relevant investigative case file.

3. Principle of Purpose Specification

ICE is authorized to collect information under Section 701 of the USA PATRIOT Act; 6 U.S.C. § 112; 8 U.S.C. §§ 1105, 1103(a)(4), 1357(a) and (b); and Executive Order 13388. Pursuant to the Homeland Security Act of 2002 (HSA), as amended, Pub. L. 107-296, 116 Stat. 2135 §§ 102, 403, 441 (Nov. 25, 2002), the U.S. Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include laws contained in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this enforcement authority to the Director of ICE in DHS Delegation Order No. 7030.2, Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (Nov. 13, 2004), and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003). Through these statutes and orders, ICE has broad legal authority to enforce an array of federal statutes including responsibility for enforcing customs authorities and federal criminal authorities.

As noted previously, this Privacy Impact Assessment addresses ICE's operational use of publicly available information, including social media information to identify, investigate, locate, arrest, and support prosecution of individuals suspected of violations of laws.

Privacy Risk: There is a risk that ICE may use publicly available information including social media information for purposes beyond what is described in this Privacy Impact Assessment.

Mitigation: This risk is mitigated. ICE mitigates this risk through training, privacy compliance processes (e.g., Privacy Threshold Analysis), auditing, and oversight. ICE Privacy has created mandatory training and rules of behaviors for ICE personnel that detail the restraints and safeguards outlined in this Privacy Impact Assessment. Additionally, new tools used to collect and use publicly available and social media information must be submitted to ICE Privacy and the DHS Privacy Office for review to ensure that the proposed use and function comply with DHS social media policy and this Privacy Impact Assessment. Prior to adoption of a new tool to access, collect, use, and maintain publicly available information, including social media information to support ICE law enforcement investigations, an ICE program or office must document the purpose of the tool's use through the Privacy Threshold Analysis process. At that time, any restrictions on its use to safeguard privacy may be set by ICE Privacy or DHS Privacy. Further, ICE supervisors audit ICE case files to ensure that the source of data and the use of publicly available and social media information in law enforcement investigations complies with the principles stated in this Privacy Impact Assessment. ICE personnel who operate in contravention to the relevant rules of behavior and this Privacy Impact Assessment will have their access to tools used on publicly available information, including social media information, online research identities revoked, and could potentially face disciplinary action.

Privacy Risk: There is a risk that the use of certain keywords or recurrent query tools to collect and use publicly available and social media information may be inconsistent with ICE's authority to collect such information.

Mitigation: This risk is partially mitigated. Any information sought through keyword queries must have a direct nexus to an authorized law enforcement investigation or activity. Further, any keywords used to query publicly available information will be designed in such a way as to not profile, target, or discriminate against any individual for lawfully exercising their First Amendment rights. To ensure that keyword searches are conducted in an authorized manner, keywords used to query publicly available information, including social media information, will be documented and may be periodically reviewed by the Office of the General Counsel, ICE Privacy, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties. Additionally, ICE Privacy will meet monthly with the respective program to assess how keywords are being used to ensure compliance with this Privacy Impact Assessment and DHS and ICE policies.

Privacy Risk: There is a risk that ICE will use a third-party vendor or contractor to collect publicly available information that it otherwise would not be authorized to collect.

Mitigation: This risk is mitigated. ICE may not use a vendor or contractor to collect, use, maintain, or disseminate personally identifiable information that ICE does not have the authority to collect, use, maintain, or disseminate. Prior to collection, ICE ensures vendors do not collect First Amendment protected information on their behalf by providing to the vendor guidelines on permissible and prohibited collection activities. After collection, ICE personnel routinely conduct oversight of any information collected by an ICE vendor or tool to ensure the information has a direct nexus to an open investigation, is accurate, and does not run afoul of any First Amendment protections.

4. Principle of Data Minimization

ICE will collect only the minimum amount of personally identifiable information necessary and relevant to an ICE law enforcement investigation and safeguard that personally identifiable information as required by law, regulation, and/or Department or ICE policy. Further, information found on a publicly available website or social media platform that is used in an investigation will be saved in appropriate case files and ICE systems, including information about which vendor the information was first identified (if applicable). The data will be maintained in accordance with the relevant Systems of Records Notice(s) and Privacy Impact Assessment(s), as well as the NARA-approved retention schedule(s). Relevant case files and case systems are periodically audited by supervisors and the ICE Records and Information Management Unit to ensure proper record retention and disposition.

Privacy Risk: There is a risk that ICE will collect and retain more publicly available information, including social media information, than necessary or relevant to support an open law enforcement investigation.

Mitigation: This risk is mitigated. Pursuant to ICE policy, ICE may only collect information relevant to an authorized law enforcement investigation. Because collection of publicly available information, including social media information, may implicate First Amendment protected activities, ICE personnel would not collect information about how an individual exercises their First Amendment rights "unless expressly authorized by statute, or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity" as prescribed by the Privacy Act. As previously discussed, ICE personnel document how information relates to an investigation or specific violation of law investigated and enforced by ICE prior to its collection.

Further, if ICE personnel discover that collected information is irrelevant to an open law enforcement investigation, they will not use or maintain it. Similarly, if information discovered not to be relevant was previously added to a case file, responsible ICE personnel will remove such information. Additionally, as noted previously, there are safeguards in place to ensure that targeted collection of publicly available information, including social media information, is directly relevant to an open law enforcement investigation. Supervisory approval is required before ICE users may automatically collect information from websites. And ongoing collection must be continually evaluated to ensure that only information directly related to an investigation is being collected. If the information is determined to be inaccurate, no longer credible, and/or no longer relevant, collection must end immediately, and such information may not be used or retained.

Privacy Risk: There is a risk that ICE will collect First Amendment-protected information.

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.[48] There are exceptions, however, including if the record is "pertinent to and within the scope of an authorized law enforcement activity." ICE personnel receive social media training created by ICE Privacy, ICE Office of the Principle Legal Advisor, and the DHS Office for Civil Rights and Civil Liberties on how to identify protected First Amendment activity and determine if publicly available content is pertinent to and within the scope of an authorized ICE law enforcement investigation. If the information does not meet this standard, then ICE may not collect or use it. Additionally, ICE personnel manually review publicly available information, including social media information, to assess its accuracy, credibility and timeliness and corroborate it by, for example, comparing it to other information maintained in government databases and other credible sources. ICE personnel will also determine and document the relevance of the information collected to the authorized law enforcement activity and whether it contains protected speech. ICE

[48] 5 U.S.C. § 552a(e)(7).

personnel may contact ICE Privacy and the Office of the Principle Legal Advisor to aid in this determination.

This determination will be periodically reviewed by the supervisory investigative agent to ensure ICE personnel adhere to the Privacy Act and do not collect First Amendment-protected information. Protected speech that is either not pertinent to or outside the scope of an ICE law enforcement activity must not be collected, used, and/or retained.

Privacy Risk: There is a risk that ICE use of automated collection and query tools (e.g., "scraping" tools) to support law enforcement investigations will collect information on or about individuals who are not suspected of violations of laws enforced by ICE.

Mitigation: This risk is partially mitigated. ICE's use of tools, such as recurrent query platforms or automated collection tools, is subject to the polices and safeguards discussed above, to minimize the risk of collecting information irrelevant to a law enforcement investigation and focus collections on information that is directly relevant to an ICE law enforcement investigation. Prior to a tool's implementation, an ICE program or office must document the purpose of the tool's use through the Privacy Threshold Analysis process. At that time, any restrictions on and privacy safeguards required for its use may be set by ICE Privacy or the DHS Privacy Office. Once in use, automated collection tools are only used for sites or chatrooms verified by ICE supervisors to contain information of suspected violations directly relevant to an authorized open investigation.

Similarly, ICE only uploads known suspect information to recurrent query platforms. Therefore, the returns created by these tools are designed and expected to be directly related to an open ICE law enforcement investigation. ICE does not use information about individuals who are not the targets of ICE law enforcement activities. Any returns are also assessed by ICE personnel to verify their accuracy and relevance to an ongoing ICE case. That verification is required before the data is loaded into an ICE case file or ICE case management system. Any data that is deemed irrelevant, inaccurate, and/or unreliable, is purged from the tool and may result in a determination to end collection on a designated site or platform.

5. Principle of Use Limitation

ICE personnel collect publicly available information, including social media information to support open law enforcement investigations. As discussed previously, search techniques and queries are governed by ICE and DHS policy, including applicable rules of behavior and this Privacy Impact Assessment.

ICE also uses tools, such as data aggregators, anonymizers, recurrent query platforms, and/or automated collection tools, to collect publicly available information directly relevant to an open law enforcement investigation. Some of these tools automate methods for detecting, summarizing, and graphically representing patterns of relationships between entities within the parameters discussed above. This allows ICE personnel to identify potentially criminal and fraudulent behavior directly related to a law enforcement investigation and assists them in

detecting crimes enforceable by ICE. ICE personnel will use these tools either alone or in combination to research and identify individuals, businesses, and business assets as targets of open law enforcement investigations. For every new tool that ICE plans to use, the relevant ICE program must submit a Privacy Threshold Analysis to ICE Privacy for review to ensure its use complies with law and policy and this Privacy Impact Assessment. At that time, ICE Privacy may recommend additional mitigation strategies to protect individual privacy. The Privacy Threshold Analysis must also be reviewed and approved by the DHS Privacy Office, which may also include additional privacy safeguards as a condition to use the tool.

In addition, ICE will not share personally identifiable information collected from publicly available information including social media information with third parties or external agencies unless directly related to an ICE law enforcement investigation. For example, after ICE has corroborated information and determined its accuracy, relevance, and timeliness, ICE may generate a shareable lead. Leads generated from publicly available information, including social media information may ultimately be shared with federal, state, tribal, local, and foreign law enforcement agencies, as well as relevant law enforcement fusion centers with which ICE has pre-existing information sharing agreements. ICE data may be shared only if the recipient agency has a need to know the information, sharing will further U.S. law enforcement and/or national security efforts, and disclosure is consistent with applicable law and agency policies. Sharing may be done manually by ICE personnel (e.g., via secure email or file transfer) or via system-to-system connections between ICE systems and a third-party system. Prior to sharing, ICE will ensure that the transfer is compatible with the original purpose of the collection (i.e., pursuant to a law enforcement investigation) and meets a routine use(s) of the applicable ICE system's System of Records Notice. ICE will share information outside the agency in accordance with the procedures and safeguards of the relevant ICE system in which the information is maintained, as described in the system's Privacy Impact Assessment and System of Records Notice[49] and consistent with information sharing agreements and applicable privacy safeguards.

Privacy Risk: There is a risk that ICE personnel without a legitimate need to know may access publicly available information, including social media information, including through access to a tool or database used by ICE in support of its law enforcement investigations.

Mitigation: This risk is mitigated. In addition to supervisors nominating and approving ICE personnel to use the tools discussed in this Privacy Impact Assessment, ICE personnel must apply to the ICE administrator of a tool or platform to be granted access to it. ICE supervisors must review every application before it is approved. Only authorized ICE personnel with a need to know and who have completed, and are current on, the prerequisite privacy and other training will be granted access to a tool or platform, including access to publicly available information accessed through the tool or platform. Lists of authorized users are reviewed periodically by ICE

[49] *See* the Appendix to this Privacy Impact Assessment for a list of ICE systems that contain publicly available and social media information and their associated Privacy Impact Assessments and System of Records Notices.

supervisory personnel to ensure a user's ongoing need to access the tool. Additionally, DHS Directive 110-01 requires that access authority be renewed annually consistent with annual training requirements. Access is contingent upon ICE personnel's successful completion of privacy and other training for operational use of publicly available information and social media information.

Privacy Risk: There is a risk that ICE may share information with parties who do not have a need to know or in a manner inconsistent with law and policy.

Mitigation: This risk is partially mitigated. If publicly available information, including social media information, is discovered in the course of an ICE law enforcement investigation and requires action by a federal, state, local, or international agency, ICE may share that information in a manner consistent with ICE policy and only for purposes permitted in the relevant System of Records Notice. ICE personnel are trained regarding whether information sharing is compatible with the purpose for which the information was originally collected. Personnel may also contact ICE Privacy for advice and guidance regarding permissible disclosures of personally identifiable information. Further, ICE personnel must document instances of information sharing in the relevant case file(s) and ICE case management systems. Instances of unauthorized disclosure are referred to the ICE Office of Professional Responsibility.

6. Principle of Data Quality and Integrity

There is a risk that information collected from publicly available sources, including social media information, may be inaccurate, incomplete, and/or irrelevant to an ICE law enforcement investigation. Accordingly, ICE must corroborate any publicly available information collected to support an open ICE law enforcement investigation to ensure that the information is accurate, relevant, timely, and complete. Additionally, if at any time ICE learns that it has received or is in possession of inaccurate information, it will correct, annotate, block or delete the incorrect information and will not use or disseminate the incorrect information. Further, ICE personnel may corroborate social media information with other data from public records data sources, information available in commercial and government databases, or information obtained from other governmental partners. ICE may not rely solely on information obtained from social media to take law enforcement action against any individual. ICE only uses this information to generate a possible lead and must corroborate the information before taking such action, including applying for a warrant or subpoena.

Finally, to ensure ICE is complying with the data quality safeguards articulated in this Privacy Impact Assessment, ICE, in coordination with ICE Privacy, will routinely review and audit all ICE offices that access publicly available information, including social media information as part of their law enforcement activities. Additionally, the DHS Chief Privacy Officer may choose to conduct a Privacy Compliance Review of ICE's use of publicly available information for law enforcement investigations.

Privacy Risk: There is a risk that information collected by ICE from publicly available sources, including social media sites, will be inaccurate and unverifiable.

Mitigation: This risk is partially mitigated. ICE uses traditional investigative methods to assess the accuracy and reliability of any publicly available information collected to support an open law enforcement investigation prior to generating a lead or entering the data into an ICE system. This includes using the totality of the information available and reviewing information from multiple sources, including public records data sources and government databases. To use publicly availability information, including social media information to support open ICE law enforcement investigations, ICE users must complete relevant training, including privacy training, to learn to analyze information and determine its reliability. ICE only considers corroborated information derived from social media to support a law enforcement investigative lead. ICE does not take any law enforcement action based solely on social media posts.

7. Principle of Security

ICE limits social media access to users who have completed annual social media training, show a need to access social media for their work, have agreed to specific rules of behavior associated with access to social media tools, and are approved to use it by a supervisor. All relevant publicly available information, including social media information, collected by ICE personnel will be stored in an ICE system(s) with built in audit controls. Users are granted access on a "need to know" basis. ICE operates its systems in compliance with the information security requirements of the Federal Information Security Modernization Act of 2014.

DHS/ICE policies and rules of behavior ensure appropriate online behavior and limit how information collected from the internet can be used for ICE operational purposes. Only ICE personnel whose official duties necessitate access to social media to support an open law enforcement investigation will be allowed to input information collected from publicly available sources, including social media platforms, into ICE systems. ICE supervisors monitor and approve which users are designated to collect publicly available information, including social media information, to support open law enforcement investigations, and that their training is current.

Supervisors must also monitor who is given access to tools and aggregators to collect publicly available information to support an open law enforcement investigation.

Access roles are assigned by a supervisor based on the user's job responsibilities and are reviewed periodically to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list by program managers and/or system administrators. Programs have limited numbers of accounts to access a tool, and operational needs will require a manager to transition access between and among ICE personnel needing access to a given tool. Additionally, tools are acquired on a license basis, and each instance of use must be justified each contract or option year. This is an additional opportunity for supervisors and program managers to determine which ICE personnel need access to a tool. It is incumbent upon the ICE

supervisors to maintain log files containing this information and make them available for ICE Privacy for inspection or for ICE Office of Professional Responsibility to conduct a complete audit.

ICE systems that contain publicly available information, including social media information, are restricted to personnel that have a need to know the information according to their job duties. When investigative data is imported into ICE systems, ICE personnel are required to either manually or electronically share this data with their supervisors for review.[50] ICE personnel are also required to record a description of the data being uploaded, such as source name/category and date retrieved, and the tool used to collect the information, which helps the supervisor evaluate whether the upload complies with ICE policy and helps other users better understand and evaluate the data. Supervisors are responsible for identifying any data imported into ICE systems in contravention of DHS/ICE policy. Supervisors may request that the system administrator delete any improperly uploaded data in an ICE system.

Privacy Risk: There is a risk that an unauthorized individual without a legitimate need to know may access publicly available information including social media information maintained in ICE systems.

Mitigation: This risk is mitigated. ICE system security measures are determined on a system-by-system basis, and all systems have varying degrees of access controls. Additionally, all ICE systems must abide by ICE and DHS security policies.[51] Moreover, because these systems contain law enforcement sensitive information (information that, if disclosed, could be detrimental to ICE law enforcement activities), additional scrutiny is placed upon user access restrictions in the systems to ensure that only authorized users are granted access. These systems go through security accreditations and Privacy Impact Assessments to ensure that only authorized users with a need to know will have access to data stored in the system, including social media information and publicly available data.

8. Principle of Accountability and Auditing

ICE ensures compliance with this Privacy Impact Assessment by instituting rigorous standards for training, rules of behavior, information sharing, auditing, and supervisory oversight. Additionally, rules of behaviors for ICE users of social media platforms to support open law enforcement investigations have been created in consultation with ICE Privacy and ICE Office of the Principle Legal Advisor to ensure the practices protect the privacy, civil rights, and civil liberties of individuals. ICE users who collect data from social media platforms certify annually that they have read and understand ICE policy and privacy guidance on the use of social media information.

---

[50] System specific controls are found in the system's Privacy Impact Assessment. ICE systems that contain publicly available and social media information can be found in the Appendix to this Privacy Impact Assessment, and are available at www.dhs.gov/privacy/documents-ice.

[51] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, 4300A SENSITIVE SYSTEMS HANDBOOK, VER. 13.1 (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

A mandated training program is also in place to teach ICE personnel how to properly collect information from publicly available sources, including social media platforms and to do so in accordance with ICE and DHS policies. This training is an annual requirement for ICE personnel with a need to collect personally identifiable information from publicly available sources, such as social media, for an operational purpose to support an ICE law enforcement investigation, and each user must sign a confirmation that they received and understood the training.

Most, but not all, tools used to collect publicly available information, including social media information provide auditing and accountability mechanisms, and provide a log of the date, time, user identity, and search terms that are queried. In these instances, ICE has access to the logs to ensure that the use of the systems is compliant with ICE and DHS policy. Otherwise, supervisors must create a local logging and auditing regime to mimic these requirements. ICE Privacy will work with supervisors to create appropriate logging and auditing capabilities.

ICE Privacy will develop and periodically administer an inspection mechanism to assess whether ICE's use of publicly available information, including social media information to support ICE law enforcement investigations is in compliance with the terms of this Privacy Impact Assessment. ICE Privacy will regularly evaluate the operations of program offices to ensure social media information users have completed required training and have agreed to follow the terms outlined in the corresponding rules of behavior. ICE Privacy will also assess a program's monitoring/auditing processes to ensure their efficacy and advise on best practices. Finally, ICE Privacy, in coordination with the DHS Privacy Office, through the Privacy Threshold Analysis process, will assess whether the use of publicly available information and associated tools to support ICE law enforcement investigations is consistent with this Privacy Impact Assessment and the safeguards described herein.

Additionally, ICE cybersecurity policies require personnel to use government furnished equipment for official operations. Tools that collect publicly available information, including social media information are accessed via government furnished equipment that is equipped with logging and oversight mechanisms to ensure the proper use of government IT systems. This equipment is assigned to specific ICE personnel who agree to be monitored regarding the equipment's use. Any interaction these tools may have with government furnished equipment (e.g., URL access, downloads, uploads) would therefore be logged and may be audited by ICE system administrators.

Further, audit logs are created when social media information is entered into ICE systems. Per the 2012 Morton Memorandum,[52] ICE personnel will retain any information derived from online sources in the same manner as if that content had been derived from a hard copy document or other data source (e.g., database). This includes noting the information collection or uploading the information into ICE systems prior to using the information for operational purposes.

[52] *See* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, POLICY GUIDANCE MEMORANDUM 100821.1 USE OF PUBLIC AND NON-PUBLIC ONLINE INFORMATION (2012).

Generally, such documentation would include the date, time, and name of the user who uploaded the data into the system, the origin of the information collected, such as the date the information was collected and the site(s) accessed, as well as any tool used to access the information. Automated documentation mechanisms are system-specific and are detailed in the system's respective Privacy Impact Assessment.[53]

ICE supervisors routinely check these logs and their accompanying data to ensure that the data entered does not violate ICE policy or system requirements. The electronic records are preserved and maintained in accordance with an applicable National Archives and Records Administration (NARA) General Records Schedule (GRS) or a NARA-approved agency-specific records control schedule. If the records are subject to a litigation hold, they may not be disposed of under a records schedule until further notification.

Privacy Risk: There is a risk that ICE personnel will collect publicly available information without the appropriate training or oversight.

Mitigation: This risk is partially mitigated. While the internet allows easy access to publicly available information, ICE users must follow all policies and procedures, including as discussed in this Privacy Impact Assessment before they may use publicly available information, including social media information in an ICE law enforcement investigation. This includes completing required privacy and other training, reviewing and agreeing to follow applicable rules of behavior, obtaining required supervisory approval, and making any required relevancy determinations as discussed previously. Additionally, publicly available information must be corroborated for accuracy and reliability before it may be used in an investigation, and no law enforcement action may be based solely on information obtained from social media.

Information relevant to a law enforcement investigation must be documented in the appropriate case file. Access, collection, use, and retention of publicly available information is subject to supervisor review. These checks help ensure ICE users have a need to acquire publicly available information to support an ICE law enforcement investigation and abide by ICE and DHS policy regarding training and oversight. Any user found to be using social media platforms or tools for a purpose that is inconsistent with law, regulation, or policy will have their access revoked and could face disciplinary action, in addition to deletion of the information.

Privacy Risk: There is a risk that a third-party vendor could have access to personally identifiable information ICE users input into vendor-provided tools or applications.

Mitigation: This risk is mitigated. While vendors may need to retain some administrative functions within the tools and applications, ICE will maintain control of all use restrictions and auditing capabilities, unless any additional functions assigned to the vendor are detailed in the contract and performed under general ICE supervision. Additionally, the vendor may not use personally identifiable information input into a tool or application by an ICE user to further refine

[53] For more information see the Appendix to this Privacy Impact Assessment.

or train its tools/models.

Conclusion

ICE uses publicly available information, including social media information, in its law enforcement investigations. ICE also uses tools to assist with its collection and analysis of this information. ICE ensures that individual privacy, civil rights, and civil liberties are respected by ensuring appropriate safeguards are in place for the use of this information and maintaining compliance with DHS policy for the operational use of social media. Through proper training and oversight, ICE ensures its personnel collect, use, and maintain information collected online in a lawful and responsible manner.

Responsible Officials

Peter J. Hatch
Assistant Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement

Kenneth N. Clark, Ph.D.
Assistant Director
Management and Administration
U.S. Immigration & Customs Enforcement

Approval Signature

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

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix

ICE Systems that maintain Publicly Available Information and Social Media Information for Law Enforcement Investigations

Name of System	Privacy Impact Assessment Citation	Associated System of Record Notice	Retention Schedule/Period
Student and Exchange Visitor Information System (SEVIS)	DHS/ICE/PIA-001-Student and Exchange Visitor Program (SEVP)	DHS/ICE-001 Student and Exchange Visitor Program (SEVP)	DAA-0567-2016-0004-0003. Retention Period: Destroy when no longer needed for reference or 10 years after cut off, whichever is later.
Law Enforcement Intelligence Fusion System (IFS)	DHS/ICE/PIA-007 Law Enforcement Intelligence Fusion System (IFS)	DHS/ICE-006 ICE Intelligence Records (IIRS)	N1-567-09-08 Item 1A(2) Retention Period: Destroy 75 years after cutoff, and only after verification that it is no longer needed to conduct agency business.
Significant Event Notification System (SEN)	DHS/ICE/PIA-023 Significant Event Notification System (SEN)	DHS/ICE-006 - IIRS DHS/ICE-009 - External Investigations	N1-567-2011-004 Retention Period: Destroy 75 years after cutoff.
ICE Subpoena System	DHS/ICE/PIA-027 ICE Subpoena System	DHS/ICE-009 - External Investigations	N1-567-2011-011. Retention Period: Destroy 10 years after cutoff.
National Intellectual Property Rights Coordination Center	DHS-ICE-PIA-041 National Intellectual Property Rights Coordination Center	DHS/ICE-009 - External Investigations	A retention schedule is currently under development. ICE is proposing a 5 year period for unpursued claims and a period for investigations of 25 years after the case is closed
ICE SharePoint Sites	DHS/ICE/PIA-043 SharePoint Matter Tracking Systems	SORN will be dependent on the program the SharePoint site is supporting (see PIA)	Determined by the purpose for the original collection
LeadTrac System	DHS/ICE/PIA-044	DHS/ICE-009	DAA-563-2013-0001-0006.

	LeadTrac System	External Investigations DHS/ICE-015 LeadTrac System	Retention Period: Destroy 75 years after cutoff.
ICE Investigative Case Management (ICM)	DHS/ICE/PIA-045 ICE Investigative Case Management (ICM)	DHS/ICE-009 External Investigations	N1-36-86-001 Retention Period: Destroy when 20 years old.
Pre-Adjudicated Threat Recognition Intelligence Operations Team Tracking System (PATRIOT)	DHS/ICE/PIA-052 Visa Security Program Pre-Adjudicated Threat Recognition Intelligence Operations Team Tracking System	DHS/ICE-012 Visa Security Program Records	N1-567-10-005. Retention Period: Destroy 25 years after cutoff for Visa Security Reviews without a nexus to terrorism. Destroy 75 years after cutoff for Visa Security Reviews found to be a nexus to terrorism.
Repository for Analytics in a Virtualized Environment (RAVEn)	DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment (RAVEn)	DHS/ICE-018 Analytical Records	Determined by the purpose for the original collection