Privacy Impact Assessment
for the

Immigration and Customs Enforcement Forensic Analysis of Electronic Media

DHS/ICE/PIA-042

May 11, 2015

Contact Point
Peter T. Edge
Executive Assistant Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 243-1717

Abstract

Digital evidence examination is the forensic acquisition and analysis of computer hard drives, thumb drives, cell phones, and any other data storage device obtained in the course of an investigation. The Office of Homeland Security Investigations within Immigration and Customs Enforcement (ICE) uses a variety of electronic tools to conduct criminal investigations that encompass analyzing digital media. ICE uses these tools and technologies to analyze the volume of stored digital evidence data given its rate of growth and ubiquity. ICE is conducting this Privacy Impact Assessment (PIA) because these electronic tools may be used to collect and maintain personally identifiable information (PII).

Overview

Digital evidence examination is the forensic acquisition and analysis of computer hard drives, thumb drives, cell phones, and any other data storage device obtained in the course of an investigation. Because of the increasing ubiquity of electronic media and the corresponding prevalence of digital evidence in the cases that Immigration and Customs Enforcement (ICE) investigates, specially-trained Computer Forensics Agents and Analysts (CFA) need tools to ingest and search through large volumes of electronic media and prepare the data for use throughout all stages of an investigation, including prosecution. Within the ICE Office of Homeland Security Investigations (HSI), the Cyber Crimes Center's (C3) Computer Forensics Unit helps to meet this need by making available to CFAs a variety of both free and proprietary data analysis and knowledge discovery tools. These tools can ingest and search through electronic media and extract relevant evidentiary material for use in investigations and other law enforcement activities. This information is then made available to HSI personnel who are working on the investigation, in accordance with established policies and procedures.

Electronic information is different from paper records because of its intangible form, volume, transience, and global presence. No one tool is currently available to comprehensively extract and present all relevant information from electronic data in order to meet ICE's law enforcement needs; consequently, HSI uses a number of different tools to ensure that it can fully analyze the media it has obtained.

The tools that HSI uses generally can create digital images of electronic media confiscated pursuant to a search warrant, subpoena, or summons; provided pursuant to voluntary production; or seized under border search authority.[1] HSI then employs the tools to image the media, creating a mirror copy to use as a working copy, which is critical to ensure the integrity of the underlying data on the media and its availability for verification. Once HSI images the media, it employs different tools to index the information and extract files and other data points

[1] See Section 1.1 for a list of ICE authorities to conduct forensic analysis of electronic media.

so that CFAs can easily search and analyze the extracted information. Extraction can be physical or logical. Physical extraction identifies and recovers data across the entire physical drive of a computer, without regard to the file system in which the data may appear. Logical extraction identifies and recovers files and data based on the operating system of the hardware, file systems, and applications residing on the hardware.

Once data is extracted, it must be analyzed to determine its pertinence to an open investigation or a suspected violation of law. HSI conducts searches to identify contraband or evidence within the scope of the search authority. If other contraband is located during the search that indicates a separate violation of law (e.g., a search conducted during a fraud case identifies child pornography images), HSI would seek a search warrant to expand the search authority. When ICE obtains electronic media, it is possible, and more than likely, that some of the information on the media will not be pertinent to the investigation or other law enforcement activity that prompted the acquisition in the first place. In order to determine what is pertinent, CFAs who are specially trained to conduct electronic searches and analyses must review all the information on the media to focus on what is most relevant and within the scope of ICE legal authority.

There are a number of types of analysis that can be conducted on electronic media:

1) timeframe, which can help determine when events occurred on a computer system or other device;
2) data hiding, which is used to detect and recover concealed data;
3) application and file, which may be used to correlate files to installed applications, examine the file structure of a drive, or review metadata; and
4) ownership and possession reviews, which help to identify individuals who created, modified, or accessed a file.

HSI uses a variety of tools for these types of analysis. The tools may be commercial or government off-the-shelf applications that are available to any user or that are specifically developed for and purchased by ICE. Some of the electronic tools require ICE agents to create index terms for search purposes and others have predetermined terms based on the common types of data found in electronic media. Some of the tools are useful for indexing the electronic media, although other tools extract and organize the data. All the tools are used primarily for developing evidence in connection with HSI investigations. The electronic media that ICE acquires may contain such categories of PII as names and addresses, email addresses, photographic images (in digital format), credit card information, and telephone numbers. The types of records vary from case to case, but may include sensitive personal information such as medical or financial data, records containing communications such as text messages and emails, and records of Internet activity.

ICE maintains the digital evidence that is analyzed until the investigation to which it pertains has been concluded, including any prosecution by the U.S. Attorney's Office. The original media is considered evidence and ICE keeps it in accordance with ICE chain of custody requirements. ICE retains the records associated with the analysis of forensic evidence in accordance with the DHS enterprise-wide schedule for investigative records.

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 possesses statutory authority for its investigations based on over 400 federal laws and regulations. Some of the pertinent statutes under which HSI may obtain digital evidence include:

- 8 U.S.C. § 1225(d), Authority relating to inspections;
- 8 U.S.C., § 1357, Powers of immigration officers and employees;
- 19 U.S.C. § 482, Search of vehicles and persons;
- 19 U.S.C. § 507, Assistance for customs officers;
- 19 U.S.C. § 1461, Inspection of merchandise and baggage;
- 19 U.S.C. § 1462, Forfeiture;
- 19 U.S.C. § 1496, Examination of baggage;
- 19 U.S.C. § 1582, Search of persons and baggage; regulations;
- 19 U.S.C. § 1589a, Enforcement authority of customs officers;
- 19 U.S.C. § 1595a, Forfeiture and other penalties; and
- 22 U.S.C. § 2778, Control of arms exports and imports.

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

The ICE Search, Arrest, and Seizure SORN[2] and the ICE External Investigations SORN[3] cover law enforcement investigatory records obtained and maintained by HSI. These records include, names, addresses, alien numbers, aliases, biographical information, electronic data, and reports prepared by investigators during the course of an investigation, or received from other

[2] DHS/ICE-008 Search, Arrest, and Seizure, 73 FR 74732 (Dec. 9, 2008).
[3] DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).

agencies participating in or having information relevant to an investigation. Both SORNs apply to various types of records collected, retained, and analyzed by HSI during the course of a criminal investigation.

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

Yes. The ICE Cyber Crime Center, where much of the work is conducted that involves the use of electronic tools, also participates in ICE's Continuous Monitoring Program, which provides ongoing security assessments for networks and systems.

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

DHS has developed an enterprise-wide schedule for investigative records that covers those associated with the forensic examination of electronic media and provides for retention according to Federal Rules of Evidence and applicable forensic standards. NARA approval of this retention schedule is pending.

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.

Not applicable.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

HSI agents collect electronic media in the course of their investigations, which may include computer hard drives, thumb drives, cell phones, and any other data storage devices. The media may contain a variety of categories of PII. HSI uses electronic tools to access, extract, and organize this information so that it may be searched and used for investigatory purposes. The search may look for names, addresses, cellphone or landline numbers, credit card information, specific record types, or a specific string of words or numbers. The search will be customized depending on what is needed to support an investigation. The specific PII that is accessed will

vary based on the type of electronic media imaged and the information that is stored within the media.

Some of the tools allow the data to be accessed and viewed without retaining the data, but with the possibility that query criteria be retained (e.g., the file path and access dates to a specific child pornography file encountered on the media). If legal justification is warranted, the use of different tools, which would allow for the data to be copied to government owned media, would be used.

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

ICE gathers information from electronic media obtained during the course of an ICE investigation or other law enforcement activity, or finds information publicly available on websites or other open and commercial sources. Electronic media identified for imaging is obtained from the execution of search warrants, subpoenas, or summons; by voluntary production; or is seized under border search authority. The individuals from whom this information is obtained varies depending on the investigation; however, it includes individuals who are the subjects of investigations, witnesses, informants, and members of the public. The data itself may contain information on a wide variety of individuals, including those listed above as well as victims of crimes. The legal process used to obtain the media determines the scope of information that may be extracted and analyzed.

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

ICE uses the information collected as evidence relevant to an investigation or prosecution of a U.S. immigration or customs law violation or other law enforcement activity. Results are generated for the case agent to review, analyze, and record. Publicly available data or information from commercial sources may be collected as part of this process if an agent determines that it is pertinent to an investigation or enforcement activity.

2.4 Discuss how accuracy of the data is ensured.

The original digital media is evidence, but is imaged so that the original is always available for comparisons. The mirror image becomes the working copy against which electronic tools are applied. The original media is maintained as evidence for further use if necessary. For example, in cases in which the working copy may become corrupted, a new clone can be created by re-imaging the original electronic media. ICE uses hashing to guarantee the authenticity of an original data set. Forensic evidence can be verified through the use of hashing. A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file,

based on a standard mathematical algorithm applied to the characteristics of the data set.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more data may be collected than is necessary to further an investigation.

Mitigation: It is often not possible to know in advance what information may turn out to be relevant and necessary to an investigation or other law enforcement activity and with electronic media extraneous information may be included with data that is of investigative interest. This risk is mitigated by the fact that any electronic media that is collected is acquired using a legal process, which establishes the parameters for a search and entails judicial or administrative oversight; is voluntarily shared; or is available publicly.[4] It is also mitigated by the fact that the electronic tools that are used to search copies of the media are intended to extract only that information that appears pertinent to an investigation.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ICE uses electronic tools to examine digital media in connection with ICE law enforcement investigations and activities. Agents and analysts develop search strings and other queries to apply to the digital media in order to produce a relevant result. Different tools can be used to produce different results: one tool might display an index where the relevant search terms are found in the media and another tool might extract data from deleted files or hidden partitions. The application of different tools to the same media may also lead to further relevant inquiries or facilitate the examination of hidden files.

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 purpose of the electronic tools used by ICE is to sift through large amounts of information in response to user inquiry or programmed functions in order to produce results that may be

[4] An exception to this rule is for ICE Special Agents acting under border search authority who may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the ICE guidelines and applicable laws.

analytically useful in connection with an investigation or other law enforcement activity. The tools can be used to highlight anomalies in the data, but are not used for "data mining" as that term is defined by law. Starting with a predicate that a violation of law may have occurred, ICE agents obtain electronic media pursuant to legal processes and review it using these tools to either confirm or refute the underlying suspicion of a violation. Analytical results are added to case files for further investigative use, including, as appropriate, prosecution of any violations.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that the data may be used or processed in ways that are inconsistent what is described in this PIA.

Mitigation: CFAs are responsible for the identification, use, preservation, acquisition, analysis, and presentation of electronic evidence and media. Their actions are governed by requirements specified in the ICE Computer Forensics Handbook and by federal laws, regulations, and policies that govern the acquisition, handling, and preservation of electronic evidence, including personally identifiable information. CFAs undergo extensive training on these requirements that mitigate the risk that the data will be used outside of the scope of these guidelines or in a manner that is inconsistent with this PIA.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Individual notice is provided to the individual that holds the electronic media or files in question (e.g., the owner of a computer or smartphone, a web hosting service such as Google). In some cases, moreover, acquisition may be voluntary, i.e., with consent of the owner of the media. ICE's Search, Arrest, and Seizure SORN[5] provides general notice that ICE seizes property in connection with its law enforcement investigations and activities. The External Investigations SORN[6] also provides general notice that ICE may seize electronic data.

[5] DHS/ICE-008 Search, Arrest, and Seizure, 73 FR 74732 (Dec. 9, 2008).
[6] DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).

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

If seizures of electronic media are effected through a legal process, the opportunities for consent may be limited to challenging the process by which the seizure is to be carried out during a court proceeding by defense counsel. In voluntary situations, an individual has consented, but is free to withdraw that consent. In the event information is downloaded from public websites, consent is not required because the information is available to anyone who accesses the site.

4.3 Privacy Impact Analysis: Related to Notice

Because digital media is collected either through legal process, through consent, or from publicly available sources, there is no privacy risk related to notice.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Information that is associated with the forensic examination of electronic media is covered by a DHS enterprise-wide retention schedule that is consistent with the Federal Rules of Evidence and applicable forensic laboratory standards. Retention also depends on whether the matter was prosecuted and whether there is an applicable statute of limitations for the underlying crime.

The retention schedule is pending approval by the National Archives and Records Administration (NARA). Under this proposed schedule, the retention period for forensic images and evidence varies depending on the nature of the investigation and its outcome. For cases that result in a prosecution, the original digital evidence would be retained for five years after expiration of all appeals. For cases that do not result in prosecution, the original digital evidence would be retained until the case is closed, unless the original digital evidence is required for follow up investigation, in which case it will be retained for 16 years. For open cases where there is no statute of limitations for the crime, the original digital evidence is considered a permanent record and would be preserved indefinitely according to Federal Rules of Evidence and applicable forensic standards.

5.2 Privacy Impact Analysis: Related to Retention

The DHS enterprise-wide retention schedule for investigative records establishes retention consistent with federal law and policy and with forensic standards. Accordingly, it mitigates any privacy risk.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Because the digital media that is examined using electronic tools is typically acquired in connection with a law enforcement activity, information that is accessed may be shared with other federal agencies, such as the Department of Justice in instances in which prosecutions are involved, or other state or local law enforcement agencies if joint investigations are involved. These law enforcement agencies could also include foreign law enforcement counterparts. The information shared is used to combat violations of the law, some of which may be global in scope.

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

Routine use G in ICE's Search, Arrest, and Seizure Records SORN allows for broad sharing of information for law enforcement purposes. It permits disclosure to an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, including criminal, civil, or regulatory violations. The same routine use G is included in ICE's External Investigations SORN. Other routine uses in these two SORNs also provide authority for sharing with courts, third parties, and international or foreign governmental authorities. These onward law enforcement uses and disclosures are consistent with the law enforcement purpose for which the data was collected.

6.3 Does the project place limitations on re-dissemination?

The information may be further disseminated by recipients on a need-to-know basis in

order to ensure proper investigation and prosecution of criminal violations. If evidence of a potential law violation is extracted from digital media, it may be used as necessary by the recipient to carry out its law enforcement functions, including prosecution of the violation. This could involve re-dissemination to others whose input is needed.

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

Disclosures that are made outside of ICE are typically made as a result of an ongoing investigation or other law enforcement activity, and the record of the disclosure is made in the pertinent case file. The electronic tools at issue in this PIA can record particulars about the data that is extracted, including time and date, but typically would only record information about the user of the tool, who is an ICE employee.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential privacy risk that too much information will be shared externally with the Department of Justice or law enforcement partners.

Mitigation: ICE conducts investigations of the matters within its jurisdiction and bolsters its case with evidence that is gleaned through the application of electronic tools to digital media. In the event that a prosecuting attorney from the Department of Justice or a law enforcement partner believes that some of the evidence is not needed for trial or further investigation, he or she will purge the information. The use of electronic tools, however, is intended to facilitate the extraction of appropriate evidentiary information from vast quantities of electronic media. By the time that CFAs have analyzed the resultant information and determined its relevance to a particular matter, it is likely that any extraneous information that might pose a privacy risk has been eliminated from consideration. In other words, the privacy risk from information sharing is likely to be minimal because at the stage that sharing occurs, a trained agent or analyst has made a determination that the information is relevant to the case and sharing it is warranted.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

The information that is extracted using electronic tools typically is added to a case file. Individuals seeking notification of, and access to any record about themselves that may be contained in ICE case files, including data extracted using electronic tools, may submit a request

in writing to ICE Freedom of Information Act Officer, by mail or facsimile at the following address:

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/

This right to access records is conditioned on the fact that all or some of the requested information may be exempt from access or disclosure to prevent harm to law enforcement investigations or interests. Each request for access will be considered individually.

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

Individuals may dispute the accuracy or integrity of any data used for prosecution purposes, during the judicial process. ICE may release non-exempt portions of investigative records to requesters pursuant to the FOIA, but investigative records are exempt from the access and amendment provisions of the Privacy Act. Providing individual access to investigative records or allowing them to alter the records could inform the subject 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 an investigation, to tamper with witnesses or evidence, and to 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. Individuals whose digital media is obtained pursuant to a legal process have notice because of that process and also may have the opportunity to challenge the seizure in an appropriate forum. In instances in which ICE has not acknowledged an investigative interest, an individual may have no opportunity to dispute the information until (and if) the matter is set for prosecution.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that some individuals whose data resides in electronic media or devices used by multiple persons will be unaware that their information has been obtained, and therefore unaware of the opportunity for redress.

Mitigation: This risk cannot be mitigated because even in cases in which several individuals have access to the same computer, the law only requires that one individual who has authority over the computer to consent to a search of its contents. The other individuals may not be aware of or share the desire to consent to such a search.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

Only trained CFAs and analysts are permitted to use the electronic tools covered by this PIA, and their examination of digital media is logged and audited. If external challenges are raised to the use of information gleaned from the analysis performed by electronic tools, these challenges are typically resolved in connection with the underlying investigation. Audit logs are reviewed routinely to identify suspected internal misuse of these electronic tools. Any violation is handled through the disciplinary process, which includes referral to the Office of Professional Responsibility in appropriate cases.

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

All ICE personnel, including CFAs, are required to take yearly privacy and information security training. Additionally, the agents and analysts who use electronic tools are trained on the various tools before they are provided access to use them.

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

As noted previously, only trained CFAs are permitted to use electronic tools to extract information from digital media.

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?

Any new agreements to share the results of analysis derived from use of electronic tools must be approved by the Office of the Principal Legal Advisor, with review by the ICE Privacy Officer.

Responsible Officials

Lyn Rahilly
Privacy Officer
Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security