Privacy Impact Assessment
for the

# Digital Device Location Data

July XX, 2019


**Contact Points**

**Lyn Rahilly**
**Privacy Officer**
**U.S. Immigration and Customs Enforcement**
**(202) 732-3300**

**Reviewing Official**
**Karen L. Neuman**
**Chief Privacy Officer**
**U.S. Department of Homeland Security**
**(202) 343-1717**

# Abstract

Technology developed by a loose consortium of government and public entities has recently provided the public, including global travelers, traders and migrants, precise geospatial information to allow them to understand where they are, have been and are going. While this is information is a tremendous asset for numerous legitimate purposes it also facilitates transnational crime to a degree. The advent of compact, GPS enabled, and inexpensive electronic devices, such as cell phones, fitness trackers and other devices capable of transmitting precise location information (hereinafter "digital location data") has also enabled the business community to discern the publics habits and patterns of life. This same digital location data freely provided to commercial entities by users for mutual benefit also provides insights into illicit pathways and practices of transnational criminals. By using commercially available location data which contains no Personally Identifiable Information (PII) and is provided by consent of the individual, law enforcement can also provide benefits by providing increased public safety and national security.

# Overview

As the world of information technology evolves, the techniques used by ICE and other law enforcement agencies must also evolve to identify, investigate, and prosecute criminals who often rely upon common technologies, such as easily obtainable maps and images of their environment, to commit their crimes. Failure to do so would hamper effective law enforcement and provide transnational criminals a unique ability to exploit geospatial information, ostensibly funded by U.S. Government and commercial entities for national security and peaceful purposes.

Industry is just now prepared to offer to the law enforcement global information in the extreme aggregate visually displaying patterns of travel, highlighting those movements that suggest transnational illicit activities. The commercially available digital location data has been processed to ensure the highest level of accuracy while maintaining the public's right to privacy.

Because of the unique privacy concerns raised by the digital device data, ICE has conducted this Privacy Impact Assessment (PIA) to enhance public understanding of the authorities, policies, procedures, and privacy controls related to use, retention and sharing of this data. This PIA discusses DHS's general border security mission and ICE's authorities and intent to use the data. This PIA details the process to obtain the data and what the data does and does not contain as it pertains to PII, concentrating on why ICE would need access to the information, and the policies and procedures in place to protect individuals' privacy. This PIA concludes with a privacy risk and mitigation analysis of those policies and procedures based on the DHS's Fair Information Practice Principles.[2]

*DHS's and ICE's Border Security and Public Safety Mission*

As the Nation's law enforcement investigative agency at the border ICE investigates a range of illegal activities such as child pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); and violations of immigration law, among many others. ICE also enforces criminal laws relating to national security, terrorism, and critical infrastructure industries that are vulnerable to sabotage, attack or exploitation. Also, ICE and its complimentary agency Customs and Border Protection (CBP) are uniquely charged with ensuring compliance with federal laws at the border including those preventing contraband, other illegal goods, and inadmissible persons from entering or exiting the United States.

ICE's authorities are derived from those exercised, prior to the homeland security reorganization in 2003, by the U.S. Customs Service (USCS) and the Immigration and Naturalization Service (INS). Those agencies were merged into one DHS investigative agency – renamed United States Immigration and Customs Enforcement, which retained the investigative components of USCS and INS. ICE, as the investigative agency, now work hand-in-hand at the border with other agencies to set forth a seamless

process for the international traveler and facilitation of trade while ensuring border security and public safety.

*ICE Law Enforcement Missions and Authorities*

As federal criminal investigators, ICE Special Agents are empowered to make investigative decisions based on the particular facts and circumstances of each case. The decision to use digital device location data is a typical decision a Special Agent, with possibly support from an Intelligence Research Specialist, makes as part of his or her basic law enforcement duties. However, although no additional permission is require as Special Agents they are compelled by policy to comply with protocols and supervisory approvals at further stages throughout the investigation.

*Data Description*

Digital device location data is commercially available through a vendor and consists of a geographic location and time stamp updated every 24 hours, but notably does not contain any PII. ICE gains access to this information through the purchase of subscription licenses using a web browser interface which allows the user to designate a specific search area and date and time of day to query. The ICE intelligence researcher is required to have investigative purpose to entering the query into the system, such as a known crime scene or as part of their border security mission.

The location data is obtained by the vendor with a individual's permission through the digital device's operating system location services API. On the front end, once a user has downloaded, installed, and opened a mobile app for the first time, a location API will ask for an explicit opt-in to share location data. In return for allowing access to the individual's location, mobile apps offer users certain location-based services, such as navigation, curated content, or a mobile ad based on nearby surroundings. The location service's API provides the most accurate location data available, synthesized from GPS, WiFi, and cellular signals. The location data is the highest quality location information available which is critical to ICE as it directly supports investigations and possible evidence in a court.

If a user has opted-in to share their current location, the application will acquire a latitude/longitude from the mobile device's OS. All digital device locations provided to ICE are obtained through this opt-in agreement which states (i) does not infringe third party IP rights (ii) was obtained with the appropriate consents and with compliance of all laws and regulations (iii) that it has all rights necessary to provide such data. Also, license rights permit creation of derivative works. The data source privacy policies permit sharing with 3rd parties such as the U.S. Government. No personally identifiable information is captured or stored by the vendor.

If a user has not allowed an application to use his or her current location any location data will not be collected, stored nor shared with ICE.

*Data Use*

The web-based digital device location data subscription service will provide ICE Homeland Security Investigations (HSI) Office of Intelligence a capability to obtain actionable leads from using unique digital device location analysis. The data allows HSI analysts to have insight into illicit activity patterns using online analytic tools through a subscription service and does not store any data on the ICE Network. The patented intelligence platform ensures privacy and data usage rights are appropriately obtained and maintained allowing law enforcement to see possible illicit activities without infringing on personal identifiable information. Purposes include:

1. Global Analysis of Illicit Pattern of movement; The analysis of a large sample of travel information obtained through the subscription will allow analysts a large sample size to determine frequency of travel to the U.S. South West Border from Central America, Mexico and other source countries. This data provides law enforcement a clear timeline and potential warning of major influxes of migrant or

criminal surges.

2. Strategic Analysis of Illicit Border Activities: Adaptive Transnational Criminal Organizations (TCOs) use methods to avoid inspection at ports of entry. Through the use of large numbers of aggregated cross border data it may be possible to identify illicit border crossings facilitating the transfer of drugs and other contraband into the U.S.

3. Crime Scenes Situational Awareness: Special Agents investigating a crime would like to know who was in the area of the crime at the time it was committed. The data could provide an indication that someone else was in the vicinity but identification of the individual would require additional law enforcement data sets or a subpoena or warrant.

4. Witness and Victim Statements Validation: The most sensitive use of the location data would be to collaborate victim and witness testimony concerning their whereabouts during and following a crime. The use of this data to possibly validate a victims story and identify their perpetrator would be extremely useful but requires additional safe guard to protect the victim and witness.

*Safeguards of Information by ICE*

ICE policies and procedures that safeguard this information are enforced through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files and random and routine inspections of field offices.

ICE recognizes the rights of individuals to privacy and knowledge of their whereabouts as recorded by digital devices have the capacity to store and share sensitive information without consent. It is the policy though that ICE will only obtain commercial digital location data that is expressly provided by consent by the individual in an agreement and without expectation of privacy. In addition, the data will not contain PII and any identification of the digital device owner will be pursued through approved law enforcement procedures, such as obtaining subpoenas and warrants. Special Agents violating these laws and policies are subject to administrative discipline and criminal prosecution. Further, when a Special Agent is in doubt of whether the data is obtained through lawful means, ICE policy requires the Special Agents to contact the local ICE Chief Counsel's office or the local U.S. Attorney's Office

All ICE Special Agents are required to take yearly training courses, available through the ICE Virtual University, including annual Information Assurance Awareness Training, which stresses the importance of good security and privacy practices, and Records Management Training, which stresses agency and individual responsibilities related to record creation, maintenance, use, retention and disposition.

During transmission to other federal agencies and non-federal entities for assistance, ICE takes appropriate measures to safeguard the information, to include, encrypting electronic information where appropriate, storing in locked containers, and hand delivery.

*Summary of Privacy Risks*

ICE has identified five privacy risks associated with obtaining, retention, and use of an individual's location data for law enforcement purposes to include (1) the individual may be unaware of the viewing or retention of his/her information by ICE; (2) location data may be combined with other law enforcement datasets to derive possible PII; (3) location data may be misused by ICE Agents; (4) ICE may disclose digital location data to other agencies that may misuse or mishandle it; and (5) new privacy risks may arise as the technology involved in this activity is ever-changing. The first risk is mitigated by the 100 percent use of consent opt-in agreements to obtain the information by the vendor. Particular means of mitigating risks two through four are discussed below. The fifth risk is further mitigated through the ongoing involvement of the DHS Privacy Office, and the commitment of ICE to revise and re-issue the applicable ICE directives, as well as this PIA when necessary.

**Fair Information Practice Principles (FIPPs)**

The Privacy Act of 1974 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. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer of DHS shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

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. The FIPPs account for the nature and purpose of DHS's information collection.

DHS conducts PIAs on Department practices and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. The search, detention, seizure, and retention of electronic devices through a border search is a DHS practice; as such, this PIA is conducted as it relates to the DHS construct of the FIPPs.

## 1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

*Information Policy Transparency*

When ICE does retains information derived from electronic devices, that information may be subject to the requirements of the Privacy Act. The Privacy Act requires that agencies publish a System of Records Notice (SORN) in the *Federal Register* describing the nature, purpose, maintenance, use, and sharing of the information. This PIA and the several SORNs published by DHS provide notice of the retention of PII at the border and the retention of some of the contents of electronic devices.

ICE has several SORNs that provide notice regarding the border search, detention, seizure, and retention of electronic devices and information. ICE may also maintain the information described in this PIA in one or more recordkeeping systems covered by the Alien File and Central Index System SORN[76] and the following ICE SORNs: ENFORCE/IDENT SORN;[77] Intelligence Information Records SORN;[78] and External Investigations SORN.[79]

These SORNs provide overall notice and descriptions of how ICE functions in these circumstances, the categories of individuals, the types of records maintained the purposes for obtaining and retention of the data, and the reasons for sharing such information. Any third party information that is retained from the vendor data base and maintained in an ICE system of records will be secured and protected in the same manner as all other information in that system.

If the ICE policy is modified, ICE will update this PIA to ensure the public's understanding remains current about the nature and extent of these searches, as well as the controls and safeguards that exist to protect the individual's rights. At a minimum, this PIA broadens the public's understanding of ICE's use of the commercial digital location data.

*Information Sharing Transparency*

Because notifying the individual of the sharing of information could impede an investigation or other law enforcement or national security efforts, ICE does not make the methods and sources of information fully transparent to the public. To ensure the protection of personal data without compromising the investigation, ICE have instituted strict oversight and review processes. Generally speaking, information, including PII, (b) (5) [redacted]. Where PII is disseminated to

other agencies, ICE will ensure the sharing is permissible under the Privacy Act of 1974, including whether (1) the requesting agency has an official need to know the information and (2) an appropriate routine use exists under the relevant SORN.

### 2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

The data covered by this PIA does not contain PII and which necessarily prohibits the agency from seeking consent of an individual. The participation consent is provided at the beginning of the process when the individual agrees to opt-in to the location data sharing agreement prior to using the digital device application API. The agreement states that the data may be provide to third parties and authorizes derived products. The vendor which provides the aggregated data to ICE is responsible for compliance of opt-in agreements with individual application providers.

ICE understands that participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical for agencies ICE which have law enforcement and national security missions. Divulging to the individual directly the use of data sources can implicate ongoing law enforcement investigations, or involve law enforcement techniques and processes that are highly sensitive. Providing individuals of interest access to information about them in the context of a pending law enforcement investigation may alert them to or otherwise compromise the investigation. ICE will involve the individual in the process to the extent practical given the facts and circumstances of the particular. In instances when direct individual participation is inappropriate, well-documented processes, well-trained ICE Special Agents, safeguards, and oversight will help to ensure the accuracy and integrity of these processes and information.

### 3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question, as well as 2) articulate the purpose(s) for which DHS will use the PII.

Information is authorized to be detained, retained, or seized and subsequently used by ICE to carry out its law enforcement missions under numerous authorities, including: 19 U.S.C. § 482 (Search of vehicles and persons), 19 U.S.C. § 1461 (Inspection of merchandise and baggage); 19 U.S.C. § 1496 (Examination of baggage); 19 U.S.C. § 1499 (Examination of merchandise); 19 U.S.C. § 1582 (Search of persons and baggage); 19 C.F.R. Part 162 (Inspection, Search, and Seizure); 8 U.S.C. § 1225 (Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing); and 8 U.S.C. § 1357 (Powers of immigration officers and employees).

Because ICE enforces federal law at the border, information may be obtained and retained from a traveler's digital device for a wide variety of purposes. The information will be used by ICE to conduct investigations into criminal and civil violations of laws, and to carry out the immigration laws of the United States. The information may be shared with other agencies that are charged with the enforcement of a law or rule if the information is evidence of a violation of such law or rule. Consistent with applicable laws and SORNs, information lawfully obtained by ICE may be shared with other state, local, federal, and foreign law enforcement agencies in furtherance of enforcement of their laws.

### 4. Principle of Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

All ICE policies and procedures relating to digital device location data seek to minimize the retention of information to that which is relevant and necessary to carry out the law enforcement investigative purpose.

(b) (5)

[redacted]

### 5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

*ICE Sharing of Retained Information*

As federal law enforcement agency, ICE has broad authority to share law enforcement information with other federal, state, local, and foreign law enforcement agencies in furtherance of law enforcement investigations, counterterrorism, and prosecutions.[103] To ensure retained information is used for the proper purpose, all ICE employees with access to the information are trained regarding the use, dissemination, and retention of PII. Employees are trained not to access the data source without an official need to know and to examine only that specific geographic area and information that might pertain to their inspection or investigation; access to such information is tracked and subject to audit.

Any such sharing is pursuant to a published routine use and documented in appropriate ICE systems and/or is recorded by those systems' audit functions.

### 6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

*ICE Data Quality and Integrity*

(b) (5)

[redacted]

As explained in Section 4 above (Minimization), ICE's policies and procedures are targeted toward limiting the amount of information that is held by ICE to that which is relevant and necessary for a law enforcement purpose, such as a criminal or civil investigation, or the admissibility of an alien into the United States. Information that is retained by ICE during an investigation is potential evidence that may

be used in a criminal, civil, or administrative proceeding. Therefore, ICE cannot alter the information to correct any inaccuracies without seriously compromising the integrity of the investigation and potentially violating federal evidentiary rules and rules of civil and criminal procedure.

To the extent that information that is retained may be inaccurate, untimely, or incomplete, the investigatory process is intended to identify evidence and other information that may be flawed or conflict with other information that is retained during the investigation. If the information is used as evidence in a civil or criminal prosecution, or if an individual is in immigration proceedings, rules of evidence and procedure and constitutional protections entitle the individual to certain due process protections with respect to the use of the information against him, including the ability to challenge the authenticity of the information and to call witnesses to dispute the quality or integrity of the information. These protections provide an adequate safeguard against inaccurate, incomplete, or out-of-date information that may be included in the information.

With respect to information integrity and quality issues in the context of the retention, duplication, and analysis of the information, ICE uses the most current technology available and places great importance on training its Intelligence Research Specialists in the latest analytic techniques. The information is always handled with concern for its ultimate potential use as evidence in court; as such, ICE Special Agents are very careful to preserve the quality and integrity of the information to avoid damaging their investigation. The Special Agent is also responsible to ensure the information is relevant to an investigation and if no relevant information is found, ICE only retains the information which is relevant.

ICE recognizes that persons in possession of electronic devices may not always have complete control or ownership over the device. In such cases, ICE establishes the possession of the device during the time period in question through a variety of means, including interviews, further investigation, and a forensic review of the devices if required.

### 7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

All ICE personnel with access to the data are screened through background investigations commensurate with the level of access required to perform their duties. IT system safeguards prevent unauthorized access, monitor use, and record all actions taken with respect to a traveler's electronic information.

Electronic devices and information will be maintained in and only accessible from secured systems through hardware and software devices protected by appropriate physical and technological safeguards, including password protection to prevent unauthorized access.

Finally, ICE policies and procedures that safeguard this information are enforced through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files and periodically administering audits.[108] Recognizing the inherent law enforcement aspect of these queries, to mitigate the privacy risk of obtaining and storing the information derived from digital device without the traveler's direct knowledge, ICE have strict recordkeeping, auditing, and oversight requirements. These measures provide specific guidance about obtaining and storing of the data as possible tips and leads understanding no PII is contained within the data.

### 8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

ICE is held accountable for complying with these principles Intelligence policies and directives through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files and random and routine inspections of field offices. Inspections delve in to every aspect of the ICE Special Agent's responsibilities, ranging from security of the hardware and facility, to training and recordkeeping. All ICE Special Agents are required to take yearly training courses including annual Information Assurance Awareness Training, which stresses the importance of good security and privacy practices, and Records Management Training which stresses agency and individual responsibilities related to record creations, records maintenance and use, and retention and disposition of records. Additionally, in the coming months, ICE Special Agents will be required to complete a new training course specifically focusing on ICE's Directive on border searches of electronic devices. This training will focus on ICE policies with respect to searches involving sensitive information (e.g., privileged material) and other procedural requirements and safeguards. The training is intended to reinforce Special Agents' knowledge of the ICE Directive and to serve as a reminder to treat such searches with special care.

Effective oversight and recordkeeping provide the means for verifiable accountability and ability to be audited. ICE conducts regular self-assessments to verify compliance with its responsibilities. The DHS and ICE Privacy Offices will also provide ongoing guidance on all privacy issues raised by significant or novel legal questions. Finally, the DHS and ICE Privacy Offices will participate in future decisions regarding technology advances in search techniques to ensure implementation is consistent with all the Fair Information Practice Principles, as well as privacy policies, procedures and laws. As the methods and policies of examining and detaining electronic devices evolve, this PIA will be updated, as appropriate.

## Responsible Officials

XXXXXX
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

## Approval Signature

XXXXXX
Chief Privacy Officer
Department of Homeland Security