Privacy Impact Assessment Update
for the

Acquisition and Use of License Plate Reader (LPR) Data from a Commercial Service

DHS/ICE/PIA-039(a)

December 27, 2017

Contact Points
Matthew T. Albence
Executive Associate Director
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Derek N. Benner
Acting Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-3300

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE) has procured query-based access to a vendor-owned commercial License Plate Reader (LPR) data service that stores recorded vehicle license plate data from cameras equipped with license plate reader technology. ICE uses LPR data from this service in support of its criminal and administrative law enforcement missions. In March 2015, ICE published a Privacy Impact Assessment (PIA) announcing ICE's intention to procure access to a commercial LPR database and describing the controls ICE would put in place to ensure the agency complies with privacy and civil liberties requirements when using the service. This PIA Update explains ICE's operational use of the service it has procured and describes the privacy and civil liberties protections that have been implemented by the agency and the vendor.

Overview

In March 2015, ICE published the DHS/ICE/PIA–039 "Acquisition and Use of License Plate Reader Data from a Commercial Service" PIA,[1] announcing its intention to procure access to a vendor-owned commercial LPR data service to be used by the ICE Offices of Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI). That PIA described the protective provisions that would be included in any executed contract to ensure privacy and civil liberties requirements would be implemented. ICE has now entered into a contract with a vendor to provide ERO and HSI with access to a commercial LPR database operated by a commercial partner. Under the terms of the contract, the primary vendor has clear accountability and oversight responsibility to ensure the commercial partner adheres to the requirements discussed throughout this PIA Update. (Hereinafter, the vendor and commercial partner are referred to collectively as "vendor").

LPR data assists ICE in developing and validating criminal and administrative law enforcement leads based on the location of vehicles that are associated with ICE criminal and administrative investigations.[2] ICE does not take any enforcement action against an individual based solely on the results of a query. Rather, ICE uses information from the LPR database to develop and corroborate other investigative information, including information from government systems. The commercial LPR database stores vehicle

[1] *See* DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service, *available at* www.dhs.gov/privacy.

[2] The principles and practices ICE adheres to when accessing and using LPR data are described in agency guidance titled, "Privacy Guidance: Agency Access to and Use of License Plate Reader Data and Technology", issued December 2017, from the ICE Office of Information Governance & Privacy.

license plate numbers that are recorded from cameras equipped with LPR technology. The commercial database receives data from a variety of governmental and private sources, including:

- Toll road cameras;
- Parking lot cameras;
- Vehicle repossession companies; and
- Law enforcement agencies.[3]

The vendor compiles LPR records from at least 25 states and 24 of the top 30 most populous metropolitan statistical areas[4] within the United States, to the extent that collection of LPR data is authorized by law in those jurisdictions. ICE does not contribute data to the commercial LPR database. Further, under the terms of the Contract, the commercial LPR vendor is not permitted to use any of ICE's query data, including photographs, for its own purposes or share information from ICE queries with other customers, business parties, or any other individual or entity without express permission from ICE.

Logging into the Database

ICE users (ERO officers, HSI agents, and certain support staff)[5] access the commercial LPR database via a web-based system. Before gaining access to the LPR service, ICE users must obtain a unique username and password and choose security challenge questions to assist in password recovery. Upon accessing the service, ICE users log in with their credentials and must agree to rules of behavior presented to them on a splash screen before they are permitted to query the database. ICE users must enter their username and password each time they access the LPR service, whether accessing via a computer or the mobile application.

Querying the Database

All ICE queries of the commercial LPR database are based on known license plate numbers. The data returned is limited to matches of that license plate number within a

[3] For a discussion of the information that the LPR database stores, *see* DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service, *available at* www.dhs.gov/privacy.
[4] A metropolitan statistical area is defined in the contract as: "a geographical region with a relatively high population density at its core and close economic ties throughout the area as defined by the Office of Management and Budget (OMB) and used by the Census Bureau and other federal government agencies for statistical purposes."
[5] Support staff includes Law Enforcement Specialists, Enforcement and Removal Assistants, Mission Support Specialists, and Management and Program Analysts.

defined time period. For ERO queries, all LPR queries are limited to a maximum 5-year timeframe, which is the approximate average length of time for vehicle ownership.[6] For HSI criminal investigations, the maximum timeframe will depend upon the statute of limitations for the particular crime being investigated. The service will not process any queries that do not specify a timeframe. The query interface also includes a mandatory drop-down field for ICE to select a "reason code" for the query from a pre-populated list (*e.g.*, criminal investigation).

To query the commercial LPR data service, authorized ICE users must provide a license plate number, the state of the license plate, a reason code, and the timeframe that ICE wants to query (*e.g.*, previous 90 days). ICE users must also complete a mandatory free-text field to reference the specific case for which the query was performed. This provides information for the user and, if applicable, an auditor, to determine what led to the particular query. ICE users enter identifying information about the subject into this field (*e.g.*, name and alien number), as well as any other helpful information. Finally, users must indicate whether they are entering data for themselves or for another individual. Because not all HSI agents or ERO officers have access to the commercial LPR data service, those without access may request that an ICE user query the database on their behalf. If so, the ICE user must enter the name of the agent or officer for whom the query is being entered.

An example of a query may be as follows:

- License plate number: ABC123;
- State: Pennsylvania;
- Reason code: Criminal investigation;
- Querying for self or other person: Self;
- Free-text: Subject name John Doe, case number 12345678; and
- Time frame: Previous 60 days.

Based on the above query, the commercial LPR service searches its records for license plate related information (*i.e.*, photographs and location information) on the queried license plate number over the past 60 days. No other law enforcement agency or commercial entity will have access to ICE query information. Furthermore, the vendor only retains ICE query information (including any PII) to maintain the audit log.

The commercial LPR service's mobile application also allows ICE users to query the database using photographs to auto-populate the license plate and state of registration

[6] *See* https://www.kbb.com/car-news/all-the-latest/average-length-of-us-vehicle-ownership-hit-an-all_time-high/2000007854/.

fields. When ICE users conducting an investigation in the field encounter a vehicle for which they need to query the LPR database, they can take a picture of the license plate from within the mobile application and submit the photograph as part of the query. The commercial LPR service then uses Optical Character Recognition technology to translate the license plate number and the state of the license plate, and auto-populates these two fields within the query interface. ICE users still must manually enter the other required data elements (*e.g.*, reason code, timeframe) to complete the query. Pursuant to the terms of the Contract, the vendor only retains these pictures for audit purposes, and is not permitted to include them in its database for search purposes. Additionally, data within the mobile application is automatically deleted from the user's phone after 60 days if not manually deleted sooner.

LPR Service Search Results

The search results contain two photographs of the vehicle, the nearest address of where the LPR captured the license plate, Global Positioning System (GPS) coordinates, web-based interactive maps, the nearest intersection, date and time the license plate was captured, and source of the record. The vendor reports 100% accuracy on query matches to indexed data. For example, a search for plate XYZ-1234 will always return records tagged as XYZ-1234. There is a possibility that environmental or logistical factors (*e.g.*, snow on plates, angle of camera) may cause an error in tagging. However, the requirement for two photographs in each search result serves to make any errors more readily apparent to users. Further, ICE personnel are alerted to these possibilities in training and have the ability to notify the vendor of any mistakes they discover during searching. Finally, ICE personnel are trained to verify any data they receive during the course of investigations before relying on it for enforcement purposes.

Alert lists

The Contract for the commercial LPR service requires the vendor to provide an "alert list" feature that enables users to save license plate numbers to be automatically queried against new records as they are loaded into the vendor's LPR data service.[7] Users may add a license plate to an alert list in one of two ways: 1) A user may batch upload up to 2,500 license plates to a single alert list[8] and 2) a user may assign an alert to a single license plate query, essentially creating a single plate alert list. For batch uploads, users

[7] The commercial LPR data service refers to license plates that have been added to alert lists as "Hot Plates."

[8] The system is being customized to limit ICE users to a maximum of 2,500 to comport with ICE policy. This upper limit supports operational efficiency by enabling one user to upload a large number of plates at the onset of accessing the database and/or related to different investigations at one time, and also supports larger operations, such as those run through ICE-led task forces. Alert list data is retained in audit logs, which are available to ICE personnel charged with ensuring proper use of the vendor database.

must include, at minimum, the license plate number, state of registration, reason code, and free-text field, as in single-query searches.

Users may search an alert list for a particular license plate and share alert list notifications between other ICE users involved in a case. When ICE users add a license plate to an alert list with multiple license plates or create a single plate alert list, they choose who will be notified of any positive matches (*i.e.*, single user, group of users, or agency-wide), with the default option being single user notification. When a new record in the database matches a license plate on an alert list, the commercial LPR data service sends a near real-time notification via email to the user originating the alert list and to any ICE user that has been included by the original user in the notification group.

The LPR data service also automatically flags license plates on ICE users' alert lists for de-confliction. The service will send an email alert to an ICE user who attempts to add a license plate to an alert list if the license plate number, state of registration, and reason code are an identical match to an entry on another ICE user's alert list. For example, if Officer Smith wants to add license plate number XYZ-1234, registered in Wisconsin, with "criminal investigation" as a reason code to his alert list, and Agent Jones has an alert list that contains an exact match for this search, the LPR service will send an email alerting Officer Smith that Agent Jones already has this plate on his alert list.[9] This ensures that users are appropriately coordinating on cases and not duplicating efforts.

Each license plate number on an alert list is valid for one year unless the user removes the query before its expiration. The service prompts users two weeks prior to the expiration of a license plate number and requires the user to affirmatively indicate that there continues to be an operational need to keep the particular license entry on the alert list active, or be given the option to delete the license plate from the alert list. The service grants the user one additional week after expiration to renew the entry in the alert list. If the user does not renew, the service removes the license plate number from the alert list.

All alert list activity is audited to capture: user name, date and time of the query, reason code, and user note associated with the query, as well as license plate number entry, deletion, renewal, and expiration from the alert list. Once the entry has either expired or an ICE user has removed it from the alert list, the data is no longer retained, except as part of the audit log.[10]

---

[9] There could be a valid reason why a license plate appears on more than one alert list. For example, Officer Smith may query the plate for immigration enforcement reasons, while Agent Jones is researching the plate for a criminal investigation.

[10] The audit logs referenced in the contract with the vendor are considered "records" under the Federal Records Act. The vendor is required to maintain these records on behalf of ICE throughout the life of the

Web Access and Mobile Application

Under the terms of the Contract, ICE is able to access the LPR service via the vendor's web interface and via an iOS-compatible mobile application. Both the web interface and mobile application incorporate appropriate technical, administrative, and physical security controls to protect the confidentiality, integrity, and availability of the shared data.[11]

The mobile application allows authorized ICE users in the field to:

- Query the LPR data service by entering the license plate number and state of registration (or photograph, as described above), reason code, and other required data elements;
- Add returned positive matches into the alert list;
- Have quick access and recall of any queries and alert lists associated with the user or designated user group; and
- Share alert list notifications between authorized ICE users involved in a case.

The vendor's application deletes any saved data on the mobile device after 60 days, if not already deleted manually by the user. Additionally, the mobile application conforms to all other privacy and performance requirements outlined in the Contract.

Individual Rights and Liberties

In the 2015 LPR PIA, ICE included a discussion of civil liberties concerns raised by the public, such as racial profiling, use of the technology at sensitive locations, and verifying the accuracy of LPR data before taking enforcement action.[12] ICE continues to value and abide by the relevant policies described in the 2015 PIA, as well as the December 2014 U.S. Department of Justice policy guidance entitled, *"Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity."*[13]

---

contract or for a maximum of seven (7) years, whichever is sooner. At the end of the contract, the vendor will extract, transfer, and load these records in a readable format to another storage medium or location specified by ICE. This transfer of records will occur no later than 30 days after the contract ends. After successful transfer, the vendor will ensure that all copies of the records (including any still-active alert list data) are securely deleted from all networks and storage media under its control, to include those belonging to its subcontractors, if applicable.

[11] The vendor is certified ISO 9001:2008, the internationally recognized standard for Quality Management Systems.

[12] For a full discussion of the individual rights and liberties issues raised in the original LPR PIA, *see* pp. 4, 7-9 in DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service, *available at* www.dhs.gov/privacy.

[13] *See* https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf.

ICE does not use the LPR data service to locate or track individuals who have no connection to ICE investigatory or enforcement activities. As discussed previously, ICE users may only submit queries using known license plate numbers to find information about vehicles connected to its law enforcement activities. If ICE determines that a queried license plate number does not relate to someone of interest in an ICE investigation, ICE personnel do not record, save, or print the search results for that vehicle. Furthermore, if a license plate on an alert list is determined to have no relation to a current ICE investigation, the ICE user who owns the alert list is required by policy to remove the plate.

Finally, ICE does not take enforcement action against any individual based solely on the information obtained from the vendor's LPR service. ICE personnel check the information against other investigative information, including information from government systems, before taking any action against the individual. It is critical for ICE users to compile the most accurate information in conducting a law enforcement investigation or enforcement activity, and in preparation for a criminal or administrative proceeding. Therefore it is necessary, as described below, to corroborate the LPR data prior to taking any action.

Reason for the PIA Update

This PIA is being updated for two reasons: (1) to inform the public that ICE has procured access to a commercial LPR data service; and (2) to describe the privacy and civil liberties protections in ICE's contract with the vendor.

Privacy Impact Analysis

Authorities and Other Requirements

Legal Authorities

ICE is permitted to collect commercial LPR data in furtherance of its investigative and enforcement missions under numerous authorities, including various criminal and civil provisions in Titles 8, 18, 19, 21, and 31 of the United States Code (USC), and associated DHS regulations.

System of Records Notices (SORNs)

LPR records protected by the Privacy Act of 1974 that are obtained in support of ERO's immigration enforcement mission are covered by the DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN.[14] This SORN

[14] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19, 2016).

notifies the public that data is obtained from commercial and public sources, among other sources, and prescribes permissible routine uses for the information.

LPR records protected by the Privacy Act of 1974 that are obtained in support of an HSI criminal investigation are covered by the DHS/ICE-009 External Investigations SORN.[15] The SORN notifies the public that data is obtained from commercial data aggregators, among other sources, and prescribes permissible routine uses for the information.

Data Retention

ERO Hard Copy Records: ERO users can print relevant information from the commercial LPR data service and store hard copy files in the appropriate target folder. These hard copy files are maintained for three years from the time the record was created, but longer retention is authorized if there is a justified business need (*e.g.*, ongoing investigation, pending litigation).[16] The cutoff point is the end of the calendar year in which the record was created, and the records are destroyed three years after the cutoff date.[17]

ERO Electronic Records: ERO users also enter relevant information into the narrative field in the Enforcement Alien Removal Module (EARM), a subset of the Enforcement Integrated Database (EID).[18] Records in EARM are maintained for 75 years.[19]

HSI Hard Copy Records: HSI stores hard copy records inside the relevant investigative case file. These files are retained onsite for 10 years, after which they are transferred to the Federal Records Center, and destroyed when they are 20 years old.[20] Longer retention may be authorized if there is a justified business need or if records are identified as permanent (*e.g.*, because they have historical significance).

HSI Electronic Records: HSI enters LPR-related information into the Investigative Case Management (ICM) system.[21] ICM records are in the process of being scheduled. Until there is a records schedule approved by National Archives and Records Administration (NARA), ICE will treat these records as permanent.

---

[15] DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).
[16] ERO proposed the three-year retention period because records maintained in target folders are compilations of records from other sources (*e.g.*, Alien Files, public databases, online searches) that can be recreated as needed, and are also frequently updated. As information from these sources is updated, there is an operational need for the target folders to have the most recent information to support the process of locating and arresting the target alien.
[17] NARA Records Control Schedule DAA-0567-2015-0016-0001.
[18] *See* DHS/ICE/PIA-015(b) Enforcement Integrated Database, *available at* www.dhs.gov/privacy.
[19] NARA Records Control Schedule DAA-0563-2013-0001-0006.
[20] NARA Records Control Schedule N1-036-86-001 (Item 161/3, INV-7b).
[21] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* www.dhs.gov/privacy.

Paperwork Reduction Act

Not applicable.

Characterization of the Information

With the acquisition of LPR data access from a commercial service, authorized ICE users can query the service by entering a known license plate number believed to be associated with a person of interest to ICE. If the license plate number entered by ICE matches a license plate in the LPR data service, a report is generated containing two photographs, allowing ICE to verify the license plate number and make/model of the vehicle. The vendor report also includes a map of where the vehicle was located, a satellite image, GPS coordinates for the closest address, nearest intersection of the vehicle's location, date and time the license plate was captured, and the source of the record (*e.g.*, Delaware toll road camera). Any information contained in these reports can be manually entered into EARM, ICM, or a hard copy file – in other words, incorporated into the appropriate subject or case file with other relevant information. ICE does not take any action on an individual based solely on the results from an LPR query.

All LPR information that ICE uses in its investigative and enforcement operations is obtained from the commercial vendor described in this PIA. The vendor obtains the LPR data through the sources described above.[22]

The vendor reports 100% accuracy of matches between queries and indexed results. However, the following factors could result in errors during the indexing process:

- The angle of the LPR camera;
- Impacted snow on a plate;
- The scan of a bent and/or damaged plate;
- Plates that are partially obstructed;
- Heavy snow or rain; or
- Other items outside of the vendor's control.

To ensure ICE personnel are able to determine whether query results are relevant, the terms of the Contract require that the response to a query must include at least two photographs on all hits, and must meet the following requirements:

[22] This includes toll road cameras, parking lot cameras, vehicle repossession companies, and law enforcement agencies.

- Photos must be of sufficient quality to allow the user to visually confirm the license plate and vehicle make/model in the photo are the same as what is represented in the vendor system.
- Query results must seamlessly integrate with web-based interactive maps. The printable report must show two different map views, the coordinates for nearest address and the nearest intersection.
- The vendor must provide a notification mechanism in the event ICE users identify photographs that do not match the data in their system (*i.e.*, license plate numbers or make/model mismatches).

Privacy Risk: There is a risk that the LPR commercial database could contain inaccurate information.

Mitigation: As discussed above, the vendor, which has provided similar services on a continual basis to other law enforcement agencies for more than five years, reports 100% accuracy or matches between queries and indexed results. For example, a search for plate XYZ-1234 will always return records tagged XYZ-1234. The vendor has also provided a mechanism for ICE to easily notify vendor personnel from within the query result if the results returned contain errors.[23] Finally, ICE does not take any enforcement action against an individual based solely on the commercial LPR data. ICE agents and officers are trained to verify all data and assess its relevance to their investigative and enforcement activities in light of other available data.

Privacy Risk: There is a risk that ICE collects more information than is necessary to fulfill its mission.

Mitigation: To determine whether information obtained from the commercial LPR data service is relevant to an investigation or enforcement matter, ICE users review all search results returned upon querying the database. If ICE users determine that certain records are not relevant, those records are not printed, saved, or stored. For example, some LPR images may display the environment surrounding a vehicle, which may include other drivers and passengers. ICE will not record any information or images of such individuals if they are not relevant to an investigation. As discussed below, ICE users must complete training to ensure that they use the LPR service appropriately, and are trained as law enforcement personnel to only consider and record relevant, accurate information.

[23] For example, the LPR data service indicates that it found a match for New York license plate number ABC123 on a Toyota Camry. However, the photographs returned to ICE show a Nissan Altima with a different license plate.

Uses of the Information

ICE uses information from the commercial vendor to further its investigative and enforcement missions. ICE ERO and HSI use the information to identify, arrest, and remove aliens from the United States who pose a risk to public safety or national security (*e.g.*, aliens with a criminal record, fugitive aliens, illegal re-entrants). HSI also uses the information to support its criminal investigations into national security threats, illegal arms exports, financial crimes, commercial fraud, human trafficking, narcotics smuggling, child pornography or exploitation, and immigration fraud. LPR data helps ICE develop viable leads based on the location of vehicles that are associated with ICE criminal and administrative law enforcement investigations.

ICE does not use the LPR data service to conduct electronic searches to discover or locate a predictive pattern or anomaly (*i.e.*, for purposes of data mining), and no other DHS components have assigned roles, responsibilities, or access to the vendor's LPR data service.

Privacy Risk: There is a risk that individuals may use information from the commercial LPR data service for purposes beyond what is described in this PIA.

Mitigation: All ICE authorized users must complete training on the appropriate use of the service and LPR data before accessing the commercial LPR database. Additionally, all ICE employees are required to take mandatory training for data security, privacy, information assurance, and records management on an annual basis. In addition, the vendor provides training to ICE personnel on the use of the LPR data service.

Further, each time that ICE authorized users log into the LPR data service, they must agree to ICE terms and conditions set forth in a splash screen before performing a query. The splash screen describes the agency's permissible uses of the system and data, and requires the user to affirmatively consent to these rules by clicking an online button before proceeding. The following rules apply to the splash screen:

- The splash screen appears at each logon event;
- The text on the splash screen is available to the user via a hyperlink within the main system interface (including the mobile application interface); and
- ICE users must affirm their understanding of the rules of behavior before they are able to complete the login process and commence a query.

The rules of behavior as presented to ICE users are as follows (paraphrased):

- ICE users must perform all queries using a license plate number and must provide certain information within the query to reference the specific criminal or administrative investigation for which the query was performed;
- ICE users must corroborate the information obtained from the commercial LPR database before taking enforcement action;
- ICE users are permitted to add license plates to alert lists only when they pertain to an ongoing criminal or administrative investigation;
- ICE users must remove license plates from alert lists when they no longer relate to a criminal or administrative investigation; and
- ICE users who violate the rules of behavior will be subject to penalties in accordance with ICE policy.

Finally, the vendor maintains immutable user-level audit logs on behalf of ICE that are made available to ICE Agency Managers, supervisors, or the ICE Office of Professional Responsibility (OPR) upon request. Agency Managers are federal employees responsible for:

- Adding, deleting, and managing users;
- Sending registration keys to new users;
- Maintaining user access request forms (electronic or hard copy); and
- Running usage reports within their Area of Responsibility (AOR).[24]

If ICE determines that personnel have used the system in an unauthorized manner, the user may be disciplined in accordance with ICE policy. Depending on the offense, such discipline could include revoking access to the commercial LPR database, a written reprimand, suspension, or termination of employment with ICE.

Privacy Risk: There is a risk that the commercial LPR database does not protect against unauthorized use, access, or loss of data.

Mitigation: ICE limits the number of users who are able to access the LPR data service and ensures that only those who need LPR data for their mission-related purposes are able to query the database. An Agency Manager must approve access before a user account is provisioned. Access to the LPR data service requires each user receive unique credentials for the web interface and mobile application. If users forget their password, they must correctly answer a security question before getting a temporary password to

[24] Each AOR (*e.g.*, New York City, Chicago) has a separate Agency Manager.

access the LPR data service. This helps to ensure that only authorized users are able to query the database.

Additionally, all authorized users must complete the trainings discussed previously before being granted access to the service. If the vendor discovers that an individual has used the service in an unauthorized manner, it is required to notify ICE as soon as practicable after the discovery. ICE may also request user-level audit logs if there is an indicator of unauthorized activity. Any ICE personnel who have accessed the system without authorization or who used the database in an inappropriate manner may be disciplined, which may include revoking access to the database, suspension, or termination of employment.

Further, the vendor is required to report the suspected loss or compromise of ICE data (*e.g.*, ICE user identities, audit trail data, ICE alert list data) including sensitive personally identifiable information (PII)[25] in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm, including any harm to ICE users. Specifically, the vendor must report any suspected loss or compromise of ICE data to the ICE Contracting Officer's Representative (COR) or Contracting Officer within one hour of the initial discovery, and must provide a written report to ICE within 24 hours.

Finally, the vendor is required to terminate user accounts within 24 business hours of receiving a request from ICE.

Notice

ICE previously provided notice of its intention to use a commercial LPR service in the 2015 LPR PIA, and now in this PIA Update provides a more detailed description to the public about the LPR data to which it has access using the vendor data service. Additionally, ICE SORNs provide public notice of broad categories of information that ICE collects in connection with mission-related activities.

Data Retention by the project

ICE users conducting queries may retain only the results they determine have relevance to their investigative and enforcement activities in the appropriate ICE investigative case file and/or target folder for the length of time prescribed by the applicable records schedule for that file. Once LPR data is incorporated into the appropriate ICE case file, it and other case file data may be queried and analyzed in other systems established to

[25] Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. *See* the DHS Handbook for Safeguarding Sensitive PII, at: https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.

perform analysis in order to develop leads, such as locating targets and linking cases using location information. These capabilities are described in the EID and ICM PIAs, cited to earlier in this document. Also, the vendor does not retain any ICE query information, except to maintain the audit log.

ERO Retention

If the LPR data service displays results that are useful to ERO in its immigration enforcement mission, ERO users can print this information and store hard copy files in the appropriate target folder. These hard copy records are maintained for three years from the time the record was created, at which point they are destroyed, in accordance with the applicable records schedule approved by the NARA. Longer retention may be authorized if there is a justifiable business need. If ERO users enter any of this information into EARM, those electronic records are retained in EID for 75 years.

HSI Retention

LPR records stored in HSI hard copy case files are retained onsite for 10 years, after which they are transferred to the Federal Records Center, and destroyed when they are 20 years old. Longer retention may be authorized if there is a justified business need or if records are identified as permanent (*e.g.*, because they have historical significance). LPR records stored in ICM are in the process of being scheduled. Until there is a records schedule approved by NARA, ICE will treat these records as permanent.

This update does not pose any new privacy risks related to data retention.

Information Sharing

ICE may share information obtained from the commercial LPR data service in a manner consistent with the Privacy Act of 1974 and DHS policy. Specifically, ICE may share this information with other entities such as the Federal Bureau of Investigation, U.S. Marshals Service, and state and local police departments in furtherance of criminal law enforcement investigations conducted as part of a multi-agency task force in which those entities are participating. ICE may also share with other law enforcement agencies under the routine uses described in the applicable SORNs listed herein. The Contract explicitly prohibits the vendor from sharing any information provided by ICE for its own purposes, or to share the information with other customers, business partners, or any other entity.

This update does not pose any new privacy risks related to information sharing.

Redress

The right to request amendment of records under the Privacy Act of 1974 (5 U.S.C. §552a) is limited to United States citizens and lawful permanent residents. Executive Order

No. 13,768 *Enhancing Public Safety in the Interior of the United States* (January 25, 2017) states: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.[26] This Executive Order precludes DHS from extending such rights by policy. Additionally, the Judicial Redress Act of 2015 (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of certain countries with access, amendment, and other redress rights under the Privacy Act in certain limited situations.[27]

As a result of Executive Order 13,768, DHS's "Mixed Systems Policy"[28] was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum (April 25, 2017).[29] This changes the ability of aliens to access and correct their record maintained in a system of records at DHS, such as EARM or ICM. Individuals not covered by the Privacy Act or the Judicial Redress Act may request access to their records by filing a Freedom of Information Act (FOIA) request.

The DHS Privacy Policy Guidance Memorandum makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records serves to undermine efficient decision making by DHS personnel, and can create the risk of errors made by DHS and its personnel. To that end, the Privacy Division in the ICE Office of Information Governance & Privacy accepts records amendment requests from individuals not covered by the Privacy Act of 1974.

---

[26] The full text of Executive Order 13,768 can be found here: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[27] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.

[28] The DHS' "Mixed Systems Policy" extended most Privacy Act protections to visitors and aliens whose information was collected, used, maintained, or disseminated in connection with a mixed system of records (i.e., contains PII on U.S. citizens and lawful permanent residents, and non-U.S. citizens and non-legal permanent residents). Memorandum Number 2007-1, DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.

[29] DHS Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 25, 2017) (DHS Privacy Policy), available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01. As the DHS Privacy Policy notes, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. §1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

Privacy Risk: There is a risk that individuals will be unable to participate meaningfully in the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: Because data obtained from the LPR data service is maintained for a law enforcement purpose, individuals' rights to be notified of the existence or non-existence of data about them, and to direct how that data may be used by ICE, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information would similarly interfere with the intended law enforcement use of the system. Nevertheless, the publication of this PIA Update and associated SORNs provides general notice about ICE's collection of information, and how that information is used.

Auditing and Accountability

Auditing of ICE's use of the commercial LPR database is done in two ways: (1) the vendor maintaining comprehensive audit trails; and (2) audits performed by the Agency manager, an ICE supervisor, or OPR.

The Audit Process

Any activity on the vendor's web interface or mobile application is fully auditable by ICE and cannot be disabled by the user. This includes all alert list activity. Under the terms of the Contract, the vendor must provide user-level audit reports to ICE upon request that include the following data:

- Identity of the user initiating the query or the person on whose behalf the query is initiated, if different;
- Exact query entered, to include license plate number, date limitations, geographic limitations (if applicable), reason code, and any other data selected or input by the user; and
- Date and time of query.[30]

The vendor provides the audit log in electronic form via secure transmission to ICE promptly upon request. The format of the audit log allows for ICE to retrieve user activity

[30] While results returned in response to the query are not retained in the audit logs, results would generally be able to be recreated by replicating the search using the logged query data.

by user name (or ID), query entered (*e.g.*, particular license plate), and date/time. ICE is able to export all audit reports in electronic PDF or Excel.

The vendor does not use audit trail data for any purpose other than those specified and authorized in the Contract. Furthermore, the vendor provides quarterly, or upon request, statistics based on positive hits against the number of requested searches and hit list. These reports can be run for any timeframe. The vendor maintains the audit logs for seven years. The vendor does not share the audit logs with any outside entities, including other law enforcement agencies. At the end of the Contract, the vendor will export/transfer any alert list data in machine-readable format to a storage medium or location specified by ICE within 30 days of the Contract's termination. Under the terms of the Contract, after successful transfer of these records, the vendor is required to delete all ICE data (including any audit log and still-active alert list data) from all networks and storage media under its control.

Training

Before being granted access to the vendor's LPR data service, authorized ICE users must complete training on the appropriate use of the service and LPR data. This supplements existing mandatory training required of all ICE personnel on data security, data privacy, information assurance, and records management.

The vendor provides initial training to authorized ICE users to orient personnel to the use of their system, including the "Help Desk" support related to the use, access, and maintenance of the system. The vendor also provides system training and "Escalation Procedures" for the Agency Manager, and will include procedures for resetting passwords. Finally, the vendor provides unlimited technical support to each user. Additionally, ICE requires all of its personnel who are permitted to access the commercial LPR data service to be trained on the nondiscriminatory use of the system containing the LPR data, and the agency's rules for acquiring and using the data, as described in the 2015 LPR PIA.

The vendor is required to support the comparison of user lists against training records to ensure the training requirement is met for all users. Regarding the alert list, users receive training on the importance of promptly removing license plate numbers from alert lists to avoid gathering LPR data without adequate justification. Finally, ICE personnel are trained to validate the LPR data against information in other government databases to which they have access. ICE authorized users do not take enforcement action solely based on the information they receive from the commercial LPR data service.

Access

ICE has agreed to limit the number of individuals who are able to access the commercial LPR database. Agency Managers ensure that only those who need LPR data

for their mission-related purposes are able to query the data service. Any ICE personnel who have accessed the system without authorization or who used the database in an inappropriate manner may be disciplined, which includes revoking access to the database. Additionally, in the event that an authorized ICE user no longer requires access to the commercial database (e.g., the user has left the agency), an administrator in the user's AOR will promptly request deletion of the user's account and the vendor is required to comply within 24 business hours.

Information Sharing Agreements

ICE only shares information with agencies outside of DHS consistent with the Privacy Act, the routine uses it has published in the relevant SORNs (External Investigations and CARIER), and pursuant to information sharing agreements that specify permissible uses of the data. Any agreements by which ICE may share information received from the commercial LPR data service are reviewed by the program's Information Systems Security Officer, the ICE Privacy Division, the Office of the Principal Legal Advisor, key program stakeholders, the Program Manager, and when required by DHS Policy, to DHS for formal review. ICE Memoranda of Understanding (MOUs) clearly articulate who will access the shared information and how it will be used. If the terms of existing MOUs are changed, addenda will be established and reviewed in the same manner as described above.

Responsible Officials

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

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security