# Privacy Impact Assessment

**for the**

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

**DHS Reference No. DHS/ICE/PIA-039(b)**

**May 21, 2021**

Homeland Security

## Abstract

In 2017, the U.S. Immigration and Customs Enforcement (ICE) 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 LPR technology. ICE uses LPR data from this service in support of administrative and criminal law enforcement missions. In March 2015, ICE published a Privacy Impact Assessment (PIA) announcing the intention to procure access to a commercial LPR database. In December 2017, ICE updated this PIA indicating that ICE had entered into a contract with a vendor to provide ICE Offices of Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI) access to an LPR database operated by a commercial partner.

Both the 2015 and 2017 PIAs describe privacy and civil liberties compliance through ICE-implemented controls. ICE is updating this PIA to document enhanced LPR functionality that will be available to select authorized ICE personnel, including: (i) geographic query – conducting a query with-in a specified geographic area (HSI personnel only); (ii) plate partial query; and (iii) and the mobile ap-plication with phone scan feature (collectively referred to as "enhanced LPR functionality" throughout this PIA). This update further explains ICE's operational use of these capabilities and associated privacy risks.

## Overview

Use of LPR data is an investigative technique with evolving functionality that supports ICE criminal investigations and administrative immigration enforcement efforts in furtherance of its public safety and national security missions.

In March 2015, ICE published the DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service PIA,[1] which documented ICE's intention to procure access to a vendor-owned commercial LPR data service to be used by ERO and HSI (hereinafter, the vendor and commercial LPR partner are referred to collectively as "vendor"). The PIA also described the privacy protections that would be included in any executed contract to ensure implementation of privacy and civil liberties requirements. These provisions included DHS and ICE policies on: racial profiling, use of the technology at sensitive locations,[2] and verifying the accuracy of LPR data before taking enforcement action. ICE published the 2015 PIA before

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER (LPR) DATA FROM A COMMERCIAL SERVICE, DHS/ICE/PIA-039 (2015), *available at* https://www.dhs.gov/privacy-documents-ice.
[2] *See* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT POLICY 10029.2, ENFORCEMENT ACTIONS AT OR FOCUSED ON SENSITIVE LOCATIONS (2011), *available at* https://www.ice.gov/doclib/ero-outreach/pdf/10029.2-policy.pdf.

identifying a vendor that could meet all the privacy requirements outlined in the document. ICE did not enter into a contract with such a vendor until 2017.

In December 2017, ICE published a PIA update[3] indicating that ICE had entered into a contract with a vendor to obtain access to a commercial LPR database, owned and operated by the vendor. The PIA update further explained ICE's operational use of the service and described the agency and vendor implementation of privacy and civil liberties protections.

The commercial LPR database stores vehicle license plate numbers that are recorded from cameras equipped with LPR technology. There are two primary sources of LPR data: (1) data from law enforcement owned LPR cameras; and (2) data from commercial LPR cameras. When ICE receives a query response of the LPR database, the returned data contains a photo of the license plate on a vehicle, the location of the scan, and the time of the scan from the specific camera. A variety of government and private sources provide data to the commercial database.[4]

ICE does not contribute data to the commercial LPR database in furtherance of any other agency's use. Additionally, the commercial LPR vendor is not permitted to use any of ICE's query data, including photographs, for its own purposes. The LPR vendor is not permitted to share ICE query information with third parties without ICE's express permission, including other customers, business parties, or any other individual or entity.

This PIA update discusses, ICE's use of enhanced LPR technology: (i) geographic query, (ii) partial plate query, and (iii) mobile scanning feature, discussed in detail in the "Reason for PIA Update" section below. This PIA also discusses "pattern of vehicle movement" data and LPR incidental (or collateral) image collection.

Enhanced LPR functionality enables criminal investigators with only limited information to identify suspect vehicles in furtherance of a law enforcement investigation. Enhanced LPR data assists ICE in developing and validating law enforcement leads. These leads are based on the location of vehicles that are associated with ICE administrative and criminal investigations. LPR data can be combined with other investigative methods and techniques to further develop critical evidence for prosecutions.

*Individual Rights and Liberties:*

The 2015 and 2017 LPR PIAs discussed civil liberty concerns, such as racial profiling,[5] use

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER DATA FROM A COMMERCIAL SERVICE, DHS/ICE/PIA-039(a) (2017), *available at* https://www.dhs.gov/privacy-documents-ice.

[4] These sources include: toll road cameras, parking lot cameras, vehicle repossession companies, and law enforcement agencies. Law enforcement LPR sources include: pole cameras, vehicle mounted cameras, and in-person handheld cameras.

[5] *See supra* note 3 for a full discussion of issues relating to individual rights and liberties raised by the use of the LPR service. Further, *see* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY POLICY GUIDANCE, AGENCY

of the technology at sensitive locations, and verifying the accuracy of LPR data before taking enforcement action. ICE continues to value and abide by the relevant policies described in these two PIAs, as well as the Department of Justice policy guidance.[6]

ICE will also update its agency-wide LPR privacy guidance requirements to incorporate information regarding enhanced LPR functionality. ICE continues to ensure that enhanced LPR functionality can be used consistent with restrictions on surveillance of sensitive locations and First Amendment-protected activity.

## Reason for the PIA Update

This PIA is being updated to inform the public of ICE's evolving uses of the following of commercial enhanced LPR functionalities: (i) the geographic query; (ii) the partial plate query; and (iii) updates to the mobile application. These enhancements expand how ICE will use LPR technology and access LPR data. At this time, the geographic query will only be used in furtherance of HSI criminal investigations and will not support ERO's immigration enforcement mission.

ICE's 2017 PIA indicated that all queries must include a full license plate number. With this update, ICE is outlining how authorized ICE personnel[7] can now conduct a query within a specified geographic area or by entering a partial license plate. Authorized ICE personnel may also use a mobile application to conduct queries, which permits use of a phone scanning feature. ICE is working to update its Rules of Behavior and contractual terms to reflect these changes. All other LPR functionality identified in prior ICE PIAs remains the same (e.g., audit trails, reporting, alert lists). Enhanced LPR functionality is described in more detail below.

Geographic Query

The expanded geographic query, which is only available for use in furtherance of HSI criminal investigations, includes use of multiple geographic points that form a polygon or polygonal coordinates. A map interface within the vendor's LPR database allows the user to draw polygonal shapes to define a region of interest. The geographic query allows authorized HSI users to look at a specific location and see which license plates were scanned during the specified

ACCESS TO AND USE OF LICENSE PLATE READER DATA AND TECHNOLOGY (2017), which discusses ICE's adherence to the First Amendment protections of the right to peaceably assemble, *available at* https://icegov.sharepoint.com/sites/insight/mgt/igp/privacy/Documents/Implementation-Guidance.pdf.

[6] *See* U.S. DEPARTMENT OF JUSTICE, GUIDANCE FOR FEDERAL LAW ENFORCEMENT AGENCIES REGARDING THE USE OF RACE, ETHNICITY, GENDER, NATIONAL ORIGIN, RELIGION, SEXUAL ORIENTATION, OR GENDER IDENTITY (2014) *available at* https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf.

[7] Only certain ICE personnel will be permitted to use the enhanced LPR functionality. In this PIA's Use and Access sections, ICE describes how the vendor can limit access based on the user's need to know, thereby ensuring that only authorized personnel can conduct a geographic or partial plate query.

time period. For example, if HSI knows that a vehicle involved in human trafficking is traveling between two cities on a given date, authorized personnel can draw a polygon between these locations and the vendor LPR database would return any vehicles traveling within this area during the specified timeframe. If authorized HSI personnel know additional information about the vehicle(s) of interest (such as make, model, color, or year), they can also include that information within the query to further refine the query results. Inputting these additional query terms will return fewer results, and HSI will not have to sort through vehicles that are unrelated to the investigation. HSI may also use this feature to repeatedly query an area suspected of criminal activity to determine if the same vehicle(s) have traveled within this area in the specified time frame.

Because HSI does not need a license plate number to run this query, the query results could contain multiple license plates. When the LPR database sends results back to HSI, personnel can filter the results in multiple ways (e.g., make, model, year). The geographic query is extremely useful in situations where HSI may know certain aspects of the subject vehicle (e.g., make, model, color, year, or state of registration), but does not know the license plate number. By using the geographic query feature, HSI can cull the results to identify the vehicle(s) of interest. As documented in prior LPR PIAs, HSI does not collect or retain any information on vehicles that are unrelated to an HSI investigation. The vendor maintains records that allow HSI to conduct audits of its activity, such as query terms, user ID, and records responsive to queries.

Geographic queries also include a "common plate" query feature. A common plate query allows authorized HSI personnel to analyze multiple locations to see if any license plate(s) appeared in the selected locations. This query produces a report containing a list of plates that were scanned in at least two of the selected locations. This query feature allows authorized HSI personnel to filter the query consistent with the aforementioned query filter ability (e.g., make, model, year). Further, HSI personnel also must enter a specific, limited timeframe for the query, and the vendor's data service will return vehicle information for any plates present in the selected locations during the specified time period. HSI will not take enforcement action based solely on information provided from the vendor's LPR data service. LPR data will be supplemented with other investigative information before enforcement action is taken.

HSI may use the common plate feature when investigating a drug trafficking case. For example, if HSI investigators know that certain locations are routinely involved in criminal activity, then they can draw polygons around those areas to receive a list of license plates scanned during the specified date and time. If the query results indicate that a certain vehicle was present in several of those locations, then HSI may use that information as a lead to take further action. Any plate scanned in at least two of the selected locations will be returned to HSI. HSI personnel can further filter data provided from the query to focus on any vehicles that match the description of the vehicle(s) of interest (e.g., 2017 red Toyota Camry). HSI will need to further investigate the

results of the data before taking any law enforcement action, but the common plate query feature provides HSI with an additional tool to further their criminal investigations.

Geographic queries can also reveal "pattern of vehicle movement" data. "Pattern of vehicle movement" analysis is a method of focused surveillance specifically used for documenting or understanding a vehicle's movements. This form of observation is generally done without the consent of the vehicle occupant(s). The aggregation of multiple points via a polygonal geographic query yields a "pattern of vehicle movement" or proximity to a crime scene. A pattern of vehicle movement may be more sensitive information than one fixed GPS coordinate.

A "pattern of vehicle movement" can provide a sweeping account of location information and may disclose sensitive information about the vehicle based on the vehicle's physical movements. For example, these queries can reveal excessive information outside the scope of an investigation, and could potentially indicate otherwise lawful activity, such as traveling to a doctor's appointment, school, or participating in a First Amendment-protected activity. HSI will not collect or retain any information on vehicles that are not relevant to an ongoing investigation, consistent with HSI's law enforcement authorities. HSI personnel are trained to focus on vehicles suspected to be involved in criminal activity. ICE analyzes the "pattern of vehicle movement" privacy risk, below, in the Characterization of the Information section.

Partial Plate Query

A partial plate query is used when the full license plate character sequence is inaccessible or unclear. Through a partial plate query, authorized ICE personnel could obtain matches from the vendor's LPR database even with incomplete license plate character strings. The full license plate number might be inaccessible to ICE personnel for several reasons (e.g., snow on plate, angle of camera, lack of light). A partial plate query can be particularly successful when combined with a "Make-Model" query.[8]

To conduct a partial plate query, a user enters a partial plate as well as all other required information to perform a query.[9] An example partial plate query term is "AB*123" if a user does not know that "ABC123" is the full license plate number. Query results will return all vehicles matching the characters entered by the user. If a user knows only one or two of a given plate's characters, the database may return a high volume of results. In turn, a user would be required to

[8] A "Make-Model" query is used when only a vehicle's manufacturer, or "make," and model are known—a vehicle year and or vehicle color may also be associated with a make and model. A "Make-Model" query is also available when the user conducts partial plate queries. This additional query information further narrows down the number of query results.

[9] To query the commercial LPR data service, authorized ICE personnel 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), specific case reference, subject identifying information, query for self or on behalf of another person-and this other person's name. For subject identifying information, ICE personnel enter identifying information about the subject into this field (*e.g.*, name and A-number), as well as any other helpful information.

spend significant time reviewing the returns. It therefore benefits users to enter as many license plate characters as possible. Authorized personnel further narrow the scope of their queries by including as much information as possible (e.g., make, model, year, color) in their queries.

Mobile Application Functionality with Phone Scan Feature

In 2017, ICE explored the use of a mobile application to conduct license plate queries. Since that time, ICE has not used this mobile application but instead has used a mobile-friendly version of the vendor's LPR database through a mobile device's web browser. In this PIA update, ICE is outlining its plan to use the vendor's mobile application with a new phone scanning feature ("Plate Scan Feature") in furtherance of its law enforcement mission.

Phone scanning entails using a phone's camera to scan license plates in a continuous automated manner (rather than "snapping" license plate photo images one at a time). ICE personnel with the vendor's mobile application can use this function to scan license plates whether they are inside or outside their patrol cars. Prior to this phone scanning feature, agents would have to hand write the license plate numbers for every vehicle at the scene. This would be particularly cumbersome where multiple vehicles were assembled in close proximity, such as larger parking lots.

This mobile application allows the user to scan vehicle plates. The scanned plates may be stored both on the ICE user's mobile device and uploaded to the vendor's law enforcement cloud server. The vendor software is able to match license plates scanned by ICE personnel with license plates in the vendor's database.[10] The vendor's mobile application enables license plate scanning on iOS and Android devices.

The mobile application has a mobile alert feature. Using this feature, the vendor can alert ICE in near real-time if one of the license plates uploaded through the mobile application matches a plate on an associated "alert list." This mobile feature can improve efficiency by providing law enforcement officers in the field with real-time LPR alerts when a scanned vehicle matches a plate on an alert list.

For example, HSI agents may conduct an investigation at an area with several vehicles assembled in close proximity, such as a parking lot. Agents on the scene can use the mobile scanning feature to scan all the plates that they encounter. The agents upload these plates to the vendor's database using the mobile application. Through the mobile alert feature, agents will be alerted to any plates: (i) that the agents previously put on their internal alert list; or (ii) that other law enforcement personnel identified on shared alert lists. If the query results contain vehicles that

[10] This vendor database could contain both commercial LPR data and state and local alert/hot list LPR data. Any positive match results are tagged "ICE" and would not be retained in the vendor database. Further, ICE does not share any query terms, query results, or uploaded images with any state or local law enforcement agencies or other entities with access to the vendor's database.

are not relevant to an ongoing investigation, then authorized HSI personnel will disregard the results and will not enter this information into any agency investigative records.

The mobile alert feature can enhance officer safety by alerting ICE personnel to a vehicle of interest associated with an occupant/owner who ICE has identified as having made threats against the agency or public.

The enhanced LPR functionality produces data-driven, real-time actionable intelligence. Beyond locating vehicles of interest, authorized ICE personnel can use the intelligence to more efficiently: apprehend offenders, prevent and solve crimes, improve both public and officer safety, and increase situational awareness. Enhanced LPR functionality enables criminal investigators with only limited information to identify suspect vehicles to further an investigation or solve a crime. Enhanced LPR data assists ICE in developing and validating law enforcement leads. These leads are based on the location of vehicles that are associated with ICE administrative and criminal investigations. LPR data can be combined with other investigative methods and techniques and used by authorized ICE personnel to develop critical evidence for prosecutions in furtherance of investigative and enforcement mission.

# Privacy Impact Analysis

## Authorities and Other Requirements

*Legal Authorities*

ICE is authorized 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 (U.S.C.), and associated DHS regulations.[11] For purposes of this PIA update, the only enhanced functionality that will be used in furtherance of ICE ERO's immigration enforcement authorities is the partial plate query.

*System of Records Notices (SORN)*

LPR records 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.[12] This SORN 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 obtained in support of an HSI criminal investigation are covered by the

[11] 8 U.S.C. Title 8—ALIENS AND NATIONALITY; 18 U.S.C. Title 18—CRIMES AND CRIMINAL PROCEDURE; 19 U.S. Code Title 19—CUSTOMS DUTIES; 21 U.S.C. Title 21—FOOD AND DRUGS; 31 U.S.C. Title 31—MONEY AND FINANCE.

[12] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080, (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

DHS/ICE-009 External Investigations SORN.[13] This 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 copies in the appropriate target folder. These hard copy records are maintained for three years from the end of the calendar year in which the record was created,[14] but longer retention is authorized if there is a justified business need (e.g., ongoing investigation, pending litigation).[15]

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).[16] Records in EID are maintained for 75 years.[17]

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.[18] 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.[19] ICM creates, manages, and maintains HSI Investigative Case

[13] *See* DHS/ICE-009 External Investigations, 75 Fed. Reg. 404 (January 5, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0567-2015-0016-0001, U.S. DEPARTMENT OF HOMELAND SECURITY, FUGITIVE OPERATIONS SCHEDULE, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2015-0016_sf115.pdf.
[15] ERO proposed the three-year retention period because records maintained in target folders are compilations of records from other sources (*e.g.,* A-Files, public databases, online queries) that can be recreated as needed and are also frequently updated. There is an operational need for the target folders to have the most recent information from these sources to support the process of locating and arresting the target noncitizen.
[16] See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.
[17] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0563-2013-0001-0006, U.S. DEPARTMENT OF HOMELAND SECURITY, BIOMETRICS RECORD FILE, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.
[18] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-036-86-001 (Item 161/3, INV-7b) , U.S. DEPARTMENT OF HOMELAND SECURITY, INVESTIGATIVE CASE FILE SCHEDULE , *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.
[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ICE INVESTIGATIVE CASE MANAGEMENT (ICM), DHS/ICE/PIA–045 (2016),

Files. The records in this system are retained in accordance with the Legacy Investigative Case File Records Schedule (N1-36-86-1-161.3/Inv.7b).[20] Investigative case files are temporary with a retention of 20 years for all HSI case category investigative cases with the exception of the case category 03 Neutrality Investigative Case File.[21]

Vendor Retention of ICE Data: ICE does not contribute data to the commercial LPR database and the vendor is not permitted to use any of ICE's query data, including photographs, for its own purposes. ICE query data is not retained by the vendor except to maintain audit logs for use by ICE.

**Characterization of the Information**

In the 2017 PIA and in ICE's contract with the vendor, ICE was required to enter a full license plate number to perform a query. If the license plate number matched a license plate in the LPR data service, then the vendor sent corresponding information back to ICE. This PIA update outlines the removal of the requirement of inputting a full license plate number and discusses how authorized ICE personnel can query the database using either a partial plate or a geographic query.

These new query capabilities alter the way that ICE collects, uses, and shares information. First, the geographic query changes how authorized personnel can query the vendor's LPR data service. Instead of entering a full license plate number, HSI personnel can instead draw polygons around the map to look for vehicles in a particular region of interest. A query using a full license plate number would return information pertaining to a specific vehicle. However, the geographic query will likely return multiple results, requiring ICE personnel to use other investigative methods to identify the subject vehicle(s).

Second, the partial plate query permits ICE personnel to query for a subject vehicle when they don't know the full license plate number. For example, a user may enter "XY*7*9" for license plate "XYZ789." The vendor LPR database would return any plates matching the pattern submitted by ICE. Submitting a partial plate number likely results in multiple vehicles being returned. ICE personnel are trained to enter as many characters as possible to increase the likelihood that the query results are narrowly tailored to the vehicle(s) of interest. In addition, a partial plate query also requires entering all other information necessary for a full plate query (e.g., state of registration, reason code).

Third, the mobile application scanning feature permits ICE personnel to scan an increased number of assembled (e.g., parked) license plates in a short time period (see "Mobile Phone

*available at* https://www.dhs.gov/privacy-documents-ice.

[20] See Legacy Investigative Case File Schedule: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf, page 44.

[21] See Neutrality Records Schedule: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf, page 58.

Scanning Overcollection" subsection below for more details). Until this capability was implemented, ICE personnel had to either write down each plate number by hand or take individual photographs of relevant license plates before running a query. This could be a time-consuming process requiring significant resources. Now, if ICE personnel see several cars parked in an area near a crime scene or an area of suspected criminality within ICE's legal authorities, they can use the mobile scanning feature to scan multiple plates at once. The versatile nature of mobile devices offers law enforcement personnel access to information not accessible by LPR cameras mounted on poles or vehicles (e.g., a handheld mobile device can fit in hard to reach places which a vehicle mounted camera could not access). At this time, the mobile feature will be used in support of criminal investigations, not for immigration enforcement matters. Should this change, ICE will update this PIA before any changes occur.

Since the 2017 PIA, there have been no changes to: (i) categories of individuals for whom the data is collected; (ii) why the information is collected; (iii) information sources; (iv) how the information is checked for accuracy; and (v) the legal authorities under which ICE can collect the information.

**Privacy Risk:** There is a risk that enhanced LPR technology query results might contain inaccurate information, leading ICE to rely on inaccurate data in furtherance of its law enforcement mission.

**Mitigation:** The risk is partially mitigated. To ensure accuracy of information, the response to a query must include at include at least two photos of all matches. Since 2017, the vendor uses high definition (HD) cameras that provide higher quality images. This results in increased accuracy of license plate matches. As mentioned in the 2017 PIA, the vendor has provided a mechanism for ICE to easily notify vendor personnel from within the query result if the results returned contain errors. Finally, ICE does not take enforcement action against any individual based solely on the information obtained from the vendor's LPR service. Authorized ICE personnel receive training to verify all accessed data is relevant to ongoing investigative and enforcement activities.

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/debris on a plate; the scan of a bent and/or damaged plate.

**Privacy Risk:** There is a risk that the system collects more information than is necessary for the purposes of the program. The following new enhancements can contribute to overcollection: (i) extraneous "pattern of vehicle movement" not relevant to an ongoing investigation; (ii) the potential for identification of individual humans (in close proximity to or associated with vehicles) whose images are captured through LPR camera technology; [22] and (iii) the increased access to information

[22] LPR images can display the environment surrounding a vehicle, which may include other drivers and passengers.

afforded by the mobile phone scanning application.

**Mitigation:** The risk is partially mitigated. To determine whether information obtained from the commercial LPR data service is relevant to an investigation or enforcement matter, ICE personnel review all query results returned upon querying the database. If ICE personnel 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. Authorized ICE users will only consider information pertaining to the vehicle (e.g., make, model, license plate number) and use that information to identify associated individuals in furtherance of its law enforcement efforts. ICE personnel must crop images containing individuals before the images are added to a case file unless the images pertain to individuals who have a known or suspected association to a criminal investigation.[23]

The enhanced LPR functionality queries (e.g., geographic query) can return information on multiple vehicles that do not pertain to an HSI investigation. HSI trains its authorized agents to only take follow-up action on relevant vehicle information in furtherance of an ongoing investigation. HSI personnel are prohibited from collecting records without a specific, articulatable target (e.g., individual or vehicle) or targeted criminal activity within the purview of HSI's authorities. As discussed below, HSI agents must complete training to ensure that they use the LPR service appropriately. As authorized law enforcement personnel, HSI agents are also trained to only consider and record relevant, accurate information. HSI agents are further trained to include as much information as possible when querying the database to narrow the query results scope (e.g., make, model, color, year). When fewer query results are returned, HSI personnel are more likely to identify the vehicle(s) of interest to promote efficiency.

*Pattern of Vehicle Movement Overcollection*

A "pattern of vehicle movement" can reveal extrinsic information not relevant to an investigation. To mitigate the return of extraneous "pattern of vehicle movement" data, HSI administrators monitor data usage for any unusual query patterns or suspicious use of "pattern of vehicle movement" data, which may be accessed in violation of HSI's Rules of Behavior for using the technology. The vendor provides audit logs quarterly, or upon request, to HSI for further monitoring of HSI's use of the enhanced LPR functionalities.

---

An LPR image may capture an individual whom ICE believes may be of interest to an investigation. For example, in a child exploitation case, ICE could run facial recognition technology on that individual (e.g., subject or victim) in accordance with prescribed policies/procedures. For more information, see previous version of the LPR PIA, *supra* note 3.

[23] Depending on the resolution of the specific LPR device, it may be possible to identify the occupants of the vehicle. However, this vendor service does not deploy facial recognition or any other technology to support automated photo identification.

As noted herein, HSI agents are trained to only consider information relevant to a potential or ongoing investigation. If information returned to HSI reveals "pattern of vehicle movement" that does not further HSI's law enforcement mission, then HSI will not collect, use, or retain such information. HSI must corroborate any "pattern of vehicle movement" data prior to taking enforcement action against a vehicle's occupants or associated individuals.

In using the geographic query function, HSI recognizes that the LPR data service may also return information on a large number of vehicles, the majority of which are not pertinent to a criminal investigation. To guard against this risk, HSI criminal investigators and analysts receive training to narrowly tailor their queries to the specific geographic area of interest. If HSI knows that a certain crime is occurring at a specified location (e.g., stash house), it would not be useful to draw a polygon around an area larger than the block where the house is located. Doing so would cause HSI personnel to spend significant time sifting through records for vehicles that have no relevance to a criminal investigation. If HSI personnel try to query an extremely large area, the vendor's database sends a warning message indicating that an excess number of records will be returned.

*Overcollection of Information on Individuals Incidental to Queries to LPR Data Service*

Authorized ICE personnel can query the vendor's LPR data service in one of three ways: (i) conducting a geographic query (HSI personnel only); (ii) entering a full or partial license plate number; or (iii) uploading photographs of subject license plates.

If ICE personnel upload photographs of license plates to the vendor's LPR database, the submitted images could display the environment surrounding a vehicle, which may include drivers and passengers. If the enhanced LPR functionalities collect collateral images of individuals in the background, in addition to vehicles, the same general overcollection risk mitigations apply as outlined in the 2017 PIA update. ICE personnel can also crop the images so that only the vehicle and corresponding license plate are captured. ICE personnel must adhere to the previously cited ICE LPR policy guidance which states that ICE will not engage in the overcollection of LPR data. ICE will not record any information or images of such individuals if they are not relevant to an investigation. Further, ICE trains its personnel to avoid drawing excessively large polygons[24] yielding numerous query results. The vendor's database will also provide a warning message to users if ICE's queries would return an excessively large number of results.[25] ICE's standard

[24] The LPR database allows for areas as small as three-square meters to be queried. However, ICE personnel are trained to query areas that return the most applicable and relevant results, drawing polygons not too large and not too small so as to narrow the focus as much as possible on the relevant amount of data to review applicable to the query. The previously referenced Rules of Behavior and training further help to mitigate this risk.

[25] The vendor's database will provide a warning message for any queries for which 10,000 or more results will be returned. This could be the result of an overly broad geographic query or a query with a timeframe which would return excessive results. If ICE receives this message, the query can still be run, but the database will produce the 5,000 most recent results. Users must confirm they would like to run a search that yields such voluminous results.

practice is to narrow a query by including as much information as possible (e.g., make, model, year, color). As noted herein, ICE users must complete, and stay current on, training to ensure that they use the LPR service appropriately; users are trained to only consider and record relevant, accurate information in furtherance of its law enforcement investigations.

*Mobile Phone Scanning Overcollection*

Mobile phone versatility allows authorized ICE law enforcement personnel to access LPR data that pole/vehicular mounted cameras cannot reach. Thus, mobile phones have increased information access, which increases the risk of overcollection.

To mitigate this risk, mobile phone access is strictly controlled. Any data transmitted via a mobile phone is subject to auditing by ICE administrators to ensure adherence to the program requirements. These audits are conducted at least quarterly, or more frequently upon request by ICE. If a user is suspected of misusing the database or performing queries unrelated to ICE's authorities, ICE can audit that user's activities and implement disciplinary measures, as necessary. Additionally, scanning large areas is counter to ICE's mission and any scanned data deemed not relevant to an ongoing investigation must be deleted. Further, authorized ICE personnel must: complete, and stay current on, training on the appropriate use of LPR data; agree to the Rules of Behavior at the login splash screen; adhere to the ICE sensitive locations policy; and abide by the terms and conditions of ICE's contract with the vendor.

**Uses of the Information**

The underlying uses of information outlined in the 2017 PIA remain the same—supporting ICE criminal and administrative law enforcement investigations. The new enhancements provide ICE the industry standard in actionable intelligence to improve public safety and assist in ICE's law enforcement mission.

Under the conditions outlined in both the 2017 PIA and the ICE Rules of Behavior, ICE users had to query the LPR database using a full license plate number. Any results returned to ICE would only pertain to that vehicle. Now, authorized users have multiple query options, some of which may return information on several vehicles (i.e., geographic queries and partial plate queries). In addition, mobile devices are a new point of collection and conduit for yielding potential matches.

**Privacy Risk:** There is increased risk that authorized ICE users may use information from the commercial LPR data service for purposes beyond what is described in this PIA. Specifically, there is a risk that ICE users will use the LPR query service to receive information on vehicles that are not relevant to an ongoing law enforcement investigation.

**Mitigation:** The risk is partially mitigated. Several of the associated risk mitigations remain unchanged from the 2017 LPR PIA (e.g., training, terms and conditions, splash screen,

user-level audit logs, discipline for unauthorized use). These mitigation strategies also apply to the new query capabilities described in this PIA update.

ICE has also taken measures to mitigate the risk that ICE could persistently track vehicles that are unrelated to a law enforcement investigation. The following controls ensure that ICE only pursues vehicles that are of law enforcement interest.

For example, ICE personnel must abide by the policies outlined in the ICE Code of Ethics, ICE agency-wide LPR guidance,[26] the Rules of Behavior appearing as a splash screen upon login, and all privacy controls outlined in ICE's original 2015 License Plate Reader PIA and the 2017 PIA update.

Further, HSI's use of data derived from LPR technology must be associated with an ongoing investigation, target of investigation, and/or targeted law enforcement activity. When HSI personnel query by geographic location, they must enter both a "Reason Code" (e.g., criminal investigation) and complete a free-text field outlining the justification for the query, which may include the applicable case number. System administrators and/or HSI agency managers audit and monitor HSI LPR use for impermissible tracking data (see Auditing and Accountability section, below). This oversight helps to ensure that LPR data is only used for purposes outlined in this PIA (and previously-published ICE LPR PIAs), the ICE agency-wide LPR guidance, the splash screen that appears at each log-on event, and consistent with ICE's contract with the vendor.

ICE will not take enforcement action based solely on information provided from the vendor's LPR data service. LPR data will be supplemented with other investigative information before enforcement action is taken. Using the geographic query, consistent surveillance enables HSI law enforcement personnel to focus on a likely vehicle of interest. Rather than drawing large polygons on the map which potentially yield extraneous query results, HSI trains its users to enter as much information as available about the vehicle in order to produce focused and narrowly-tailored query results. HSI will never run geographic queries solely based on demographic characteristics (e.g., Little Italy or retirement community). Rather, HSI criminal investigators must establish reasonable suspicion that the queried area is associated/linked to an ongoing investigation before conducting a geographic query. The geographic query is particularly helpful in combatting smuggling and trafficking operations, which typically involve vehicles transporting humans or contraband over a wide area.

Finally, ICE has implemented the following controls to mitigate the risk of misuse. System administrators or agency/account managers ensure that those individuals without log-in credentials do not engage in unauthorized use. Toward this end, administrators restrict unauthorized personnel from running certain queries, such as geographic or partial plate queries. ICE personnel can be

[26] See *supra* note 5.

disciplined if they use the LPR service for unauthorized purposes. This action includes revocation of LPR access, risk of employment termination, and possible criminal prosecution.

**Notice**

ICE has not identified any new risks associated with notice. While photographs of license plates using the mobile scanning feature could incidentally include individuals not associated with an ICE investigation (collateral image), this risk was already assessed in the 2017 PIA when ICE personnel uploaded photos one at a time.

ICE does not record images which are not relevant to an investigation. If ICE determines a vehicle is relevant to an investigation, ICE may take exploratory steps. It may not be operationally feasible to offer notice to individuals captured in collateral images if ICE determines that such individual is relevant to an ongoing investigation (i.e., a subject/victim of a crime within ICE's legal purview). If ICE makes this determination, ICE would take necessary fact-finding steps such as running a facial recognition technology query on the individual.[27]

**Data Retention by the Project**

With this update, the LPR record retention policy is unchanged for both hard copy and electronic records. In addition, there is no change to how long or for what purposes the vendor may retain any information provided by ICE. The vendor only retains this information for audit purposes; no other entity with access to the vendor's LPR database can access or use information pertaining to an ICE query. Therefore, ICE has not identified any new risks regarding data retention.

[27] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES, DHS/ICE/PIA-054 (2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

**Information Sharing**

Existing LPR data sharing does not change as a result of this expanded functionality. This update does not pose any new privacy risks related to information sharing. ICE continues to develop MOUs with information sharing partners if it intends to share any LPR data outside the Department, and has executed one information sharing agreement since the publication of the prior PIA.

**Redress**

This PIA update does not change an individual's rights of access, redress, and correction.

**Auditing and Accountability**

This PIA update does not change the ICE LPR audit process. ICE has responsibility for auditing users (e.g., which users should, or should not, have LPR use and access service). These audits also help ensure that HSI users do not violate the sensitive locations policy when conducting queries (specifically, the geographic query). Audits conducted on users can detect sensitive location queries inconsistent with mission needs, thereby ensuring that ICE adheres to this policy. Contractually, the vendor audits LPR use and monitors audit logs, which it provides to ICE officials on a quarterly basis (or upon request).[28]

This PIA discusses new query features available to a subset of authorized ICE personnel. Accordingly, ICE has taken the following steps to ensure access controls are implemented.

First, the vendor will create a separate log-in point for users authorized to use the vendor's enhanced LPR functionality. ICE personnel who have not been granted this access may only query the database using a full license plate number. The approved list of personnel is subject to change based on the individual's roles and responsibilities.

Second, system administrators, or agency/account managers,[29] must ensure that those without log-in credentials do not engage in unauthorized use. Toward this end, administrators restrict unauthorized personnel from running certain queries, such as partial plate or geographic queries. Further, ICE personnel will receive disciplinary action if they use the LPR service for unauthorized purposes.

ICE system administrators can audit user activity on the vendor's web interface or mobile application. Auditing data includes the identity of the user initiating the query or the person on whose behalf the query is initiated, if different. The query interface requires a user to identify

[28] 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 query using the logged query data.
[29] The ICE system administrator(s) manages the agency's LPR service user group, including creating user accounts, managing user profiles and permissions, managing alert lists or hot lists, establishing agency data sharing relationships, setting agency data retention policies, auditing users, and ensuring compliance with agency policy.

whether the user is querying the LPR service for him or herself or for another ICE user. While ICE personnel will most commonly query the LPR service for themselves, there are a few scenarios when they perform a query on behalf of a colleague. This could occur when an HSI agent in the field is in the middle of conducting an interview of an investigation subject and cannot simultaneously query the LPR database. Unable to conduct the query him/herself, the agent may contact an HSI criminal analyst with access to the LPR database to conduct the query on the agent's behalf. Additionally, if an agent in the field does not have a mobile device on his/her person to run the query, the agent may call a colleague who otherwise has access to run the query on the agent's behalf. If the user is making the query on behalf of another individual, the query interface will require the user to enter the name of the other individual. This helps ensure that only authorized ICE personnel can use the enhanced LPR functionality. Users may be audited for suspicious query patterns (including excessively large geographic areas) associated with the geographic query function. This audit function is in line with the ICE sensitive locations policy.[30] ICE created this policy to govern enforcement actions at, or focused on, policy-defined sensitive locations. The audit function reveals suspicious query trends involving queries disproportionately directed at these sensitive locations. Through this oversight, ICE personnel who violate this policy may be disciplined for any misuse of the database.

*Training*

With this PIA update, ICE identifies a privacy risk arising with the introduction of enhanced LPR functionality. As ICE recognizes the privacy risks associated with enhanced LPR functionality, the provided training needs to be updated and expanded to address these new features.

**Privacy Risk:** There is a risk that ICE personnel may use LPR information outside the scope of this PIA update, as they do not receive sufficient privacy and civil rights/civil liberties training regarding the enhanced LPR functionalities.

**Mitigation:** This risk is partially mitigated. First, the LPR vendor provides training on the use of the tool itself, which includes data confidentiality training and specifically outlines consequences for abusing or misusing information from the LPR database. ICE is working with the LPR vendor to ensure that contractual training terms accurately reflect the enhanced LPR functionality. In addition, all ICE personnel must complete annual DHS Privacy training. LPR service users must complete, and be current on, this training to ensure they use the service appropriately and understand the privacy safeguards.

Second, all ICE personnel must agree to the Rules of Behavior, appearing as a splash screen when the user logs into the vendor's LPR database. ICE is in the process of updating the

[30] *See* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT POLICY 10029.2, ENFORCEMENT ACTIONS AT OR FOCUSED ON SENSITIVE LOCATIONS (2011), *available at* https://www.ice.gov/doclib/ero-outreach/pdf/10029.2-policy.pdf.

content of this splash screen to incorporate rules pertaining to the enhanced LPR functionalities described in this PIA update. In addition, ICE has created agency-wide guidance issued to all personnel who access LPR data. This guidance outlines the appropriate use of LPR technology, including how personnel use the vendor's database. The guidance specifically guards against the overcollection of information; reiterates ICE's policy on enforcement actions at sensitive locations; explains the prohibition on using LPR information about an individual based solely on special protections (e.g., race, religion, sexual orientation), and confirms that any ICE personnel using the vendor's database must first receive appropriate training.

Third, ICE supervisors are responsible for overseeing their employees' use of the vendor's LPR database. Supervisors monitor LPR use and would step in to halt any misuse that occurs. Serious cases of misuse would be reported to OPR, which could lead to discipline for unauthorized use.

Further, ICE is developing future privacy, civil rights, and civil liberties training which leverages its expertise in conjunction with vendor training. The combination of these two training perspectives further address training requirements to mitigate this risk. ICE will tailor this training to include privacy concerns of the enhanced LPR functionalities described in this PIA update, such as proper use of the geographic search function.

*Access*

The LPR enhancements discussed in this PIA pose new risks pertaining to access. ICE has weighed these potential risks against the benefits that they provide and has incorporated mitigation strategies accordingly. By accessing these new query functions, authorized ICE personnel increase their chances of generating leads. This access, in the form of increased actionable intelligence, improves public safety in furtherance of ICE's law enforcement mission.

The vendor uses technical controls and mechanisms within its suite of products that facilitate privacy controls on the data and restrict access to only those whom the agency grants access. The vendor's technical controls include features such as data encryption, password complexity requirements, password change rules, and other network protections.

Any ICE personnel who access the system without authorization or who use the database in an inappropriate manner will receive disciplinary action, which may include revoking access to the database, suspension, or termination of employment.

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

**Mitigation:** This risk is partially mitigated. Consistent with the 2017 PIA, ICE limits the number of users who can access the commercial LPR database. ICE ensures that only those who need LPR data for their mission-related purposes can query the database. ICE supervisors are

responsible for ensuring that their users have a need to know for the data in the LPR database in order to be granted access. Further, ICE agency managers work with the vendor to update the list of approved personnel to ensure that only authorized ICE personnel can access the database. In the context of the geographic query, this access is limited to HSI Criminal Investigators, Task Force Officers, Criminal Analysts, and Investigative Assistants who have all been fully vetted with appropriate clearances to conduct or support criminal investigations.

ICE works with the vendor to ensure that only authorized users have access to enhanced LPR functionality. ICE has responsibility for auditing users (e.g., which users should or should not have access to the product). Contractually, the vendor audits product use and monitors audit logs; the vendor sends quarterly audit reports to the ICE Contracting Officer and the Contracting Officer Representative.[31] ICE Privacy will continue to work with these offices, supervisors, and the vendor to ensure audits are carried out effectively.

ICE also ensures that authorized personnel only have access to data for which they are permitted to view. For example, LPR data returned will be limited to matches within the time period specified in the query. Authorized ICE personnel will create queries in LPR databases with specific temporal limitations; the system does not permit a query that lacks a specified timeframe. Further, HSI personnel are prohibited from drawing outsized polygons yielding an unwieldy volume of query results. Rather, ICE's standard practice requires a properly narrowed query scope by including as much information as possible in the query.

**Privacy Risk:** There is a risk that unauthorized ICE personnel can access the enhanced LPR functionality.

**Mitigation:** This risk is partially mitigated. ICE's agency-wide LPR guidance, Rules of Behavior (e.g., splash screens), and required DHS training (such as privacy training and integrity awareness training) provide policies for how personnel can use the technology. All ICE authorized personnel must complete training on the appropriate use of the service and LPR data before accessing the commercial LPR database. Additionally, all ICE personnel must agree to the Rules of Behavior, appearing as a splash screen when the user logs into the vendor's LPR database.

[31] The vendor provides auditing of all user activity for proper governance and oversight. All user queries and reports are clearly visible to agency managers for reporting purposes. The audit logs also include the user who performed the query, and the query criteria used to query the vendor's reporting network platform.

ICE will incorporate multiple account management controls relating to the way ICE personnel access the database to further mitigate the risk of unauthorized access. Consistent with this PIA's Auditing and Accountability section, the vendor can restrict access to the geographic query function to only HSI authorized personnel.

## Contact Official

Albert Giangregorio
Acting Division Chief, Transnational Organized Crime (TOC)
Office of Homeland Security Investigations (HSI)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security
(802) 872-6222

## Responsible Official

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

## Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717