Privacy Impact Assessment
for the

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

DHS/ICE/PIA-039

March 19, 2015

Contact Point
Daniel H. Ragsdale
Deputy Director
U.S. Immigration & Customs Enforcement
(202) 732-3000

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

Abstract

U.S. Immigration and Customs Enforcement (ICE) uses information obtained from license plate readers (LPR) as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions. Because LPR information can be combined with other data to identify individuals and therefore meets the definition of personally identifiable information (PII), ICE is conducting this Privacy Impact Assessment (PIA) to describe how it intends to procure the services of a commercial vendor of LPR information in order to expand the availability of this information to its law enforcement personnel. ICE is neither seeking to build nor contribute to a national public or private LPR database. In addition, through this PIA, ICE is assessing the potential impact of the use of information obtained from LPRs on the civil liberties of the public and explaining the measures to be put in place to mitigate such concerns. ICE will publish an updated PIA before the commercial solution described here becomes operational.

Introduction

As part of its criminal and civil enforcement missions, U.S. Immigration and Customs Enforcement (ICE) relies on a variety of law enforcement tools and techniques to ensure public safety and national security. One of these tools is the collection, use, and retention of data that is collected using license plate reader technology.

A license plate reader (LPR) is a system consisting of a high-speed camera, or cameras, and related equipment, mounted on vehicles or in fixed locations (e.g., bridges, toll booths, parking garages) that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device. Then, the system automatically converts the digital photographic images of license plates and associated data into a computer-readable format. This computer-readable format, also known as "a read," contains some or all of the following information: (1) license plate number; (2) digital image of the license plate as well as the vehicle's make and model; (3) state of registration; (4) camera identification (i.e., camera owner and type); (5) Global Positioning System (GPS) coordinates[1] or other location information taken at the time the information was captured; and (6) date and time of observation. Some LPR systems also capture within the image the environment surrounding a vehicle, which may include drivers and passengers. Information can be collected from all vehicles that pass the camera.

[1] GPS is a satellite-based navigation system that provides location and time information anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

A number of commercial enterprises collect LPR data from both private and public contributors, including law enforcement agencies, parking garages, and repossession companies, and make it available on a fee-for-service basis to various entities, both public and private. LPR data is stored for immediate or future queries, which may be manual or automatic. It is important to note that to query a commercial LPR database, the investigator must enter the license plate number of the vehicle he or she wants to locate.

Historically, ICE has had limited access to LPR data--both from its own cameras[2] and from commercial sources.[3] Its primary investigative offices, Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI) have each used commercial LPR information, when available, as a source of data (among other data sources) to assist in the execution of their law enforcement missions. ERO and HSI use the information to identify, arrest, and remove aliens who are immigration enforcement priorities, which at the present time include at-large aliens who have a criminal record (criminal aliens), fugitive aliens, illegal re-entrants, and those individuals posing a public safety or national security risk. HSI also uses the information in support of 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.

ICE has identified a number of benefits from the use of LPR data in its mission activities. This data can help resolve cases that might otherwise be closed for lack of viable leads, enhance both officer and public safety by enabling enforcement actions to occur in locations that minimize the inherent dangers associated with these encounters, and reduce the hours required to conduct in-person physical surveillance. Consequently, ICE is seeking to procure the services of a third-party vendor that offers a query-based LPR service to provide HSI and ERO offices with uniform access to commercial LPR data. ICE is neither seeking to build nor contribute to a national public or private LPR database. Rather, ICE is seeking an enterprise-wide commercial solution to help it more efficiently develop leads based on the location of vehicles that are associated with ICE criminal investigations and civil enforcement actions.

In defining the need for this enterprise-wide solution, ICE identified requirements that

---

[2] This PIA does not apply to ICE's use of LPR cameras to collect information directly, or its use of LPR databases available when its law enforcement personnel are detailed to other agencies, fusion centers, or task forces. ICE intends to develop policy guidance for the use of LPR information, however, which will be applicable to all such information, regardless of how it is obtained.

[3] Two ICE field offices currently have subscriptions to commercial LPR information, which are being used to support ongoing criminal investigations. Standard ICE privacy policies apply to these users. Once a vendor is selected that can provide the protections described in this PIA, ICE will terminate any pre-existing contract vehicles that lack those protections to ensure uniformity across the agency.

will guide its future acquisition of LPR information from commercial vendors to minimize the potential impact of this tool's use on individuals' rights and privacy. These requirements address issues including: the development of a mobile application that will allow ICE agents and officers to query and receive LPR data results while working in the field; time limits on search capabilities that align with ICE mission requirements; internal policy controls that ensure queries are conducted only on active cases; and strong auditing requirements. ICE also intends to develop specific user training that highlights the limitations and protections on the query and use of LPR data to promote privacy and civil liberties.

Benefits and Risks of Using LPR Data

DHS defines Personally Identifiable Information (PII) as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, employee, or contractor to the Department.[4] The use of LPR data stored in a commercial database involves PII because the license plate information is linkable to an individual.

ICE has identified a number of benefits from the use of commercial LPR data in its mission activities. Knowing the previous location(s) of a vehicle can help determine the whereabouts of subjects of criminal investigations or priority aliens to facilitate their interdiction and removal. In some cases, when other leads have gone cold, the availability of commercial LPR data may be the only viable way to find a subject. This LPR data can also show the previous movements of a subject, which may help ICE law enforcement personnel plan to apprehend a subject in a safe manner that is not near sensitive locations, such as schools. This enhances the safety of the public as well as the officers involved in questioning or detaining an individual. Commercial LPR data also allows ICE to identify connections between a car and an address known for criminal activity, which may help identify individuals involved in that activity and lead to the successful conclusion of an investigation.

The availability of an "alert list" feature in the vendor software, also known as a "hot list," by which ICE personnel can be notified shortly after a vehicle of interest is located, may help to bring about the successful and speedy conclusion of an enforcement action or investigation. ICE will only receive information in near real-time from the commercial vendor if an ICE officer adds a license plate to the "alert list."

---

[4] DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, Jan. 7, 2009 (as amended), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

The purpose of acquiring query access to commercial LPR data is not to use it in every case; in some cases no license plate information will be available to investigators to query and in other cases it may not be needed. Commercial LPR data will be used, however, when the status of an investigation or enforcement action warrants, typically when the current or past location of the subject or a vehicle is of particular interest in the case. For example, commercial LPR data is particularly useful in enforcement cases in which ICE is attempting to locate aliens who fall within ICE's stated enforcement priorities, such as criminal aliens, so ICE can arrest them and place them into removal proceedings. It is also particularly useful in the search for wanted fugitives and in certain types of criminal cases in which the specific movements of a target(s) may reveal helpful information about criminal activity, such as the movement of smuggled goods or meetings among suspects. In some cases, determining the current or past location of a vehicle may provide a useful lead that can help bring about the conclusion of a case.

This PIA is intended to establish the parameters of ICE's use of LPR data acquired from a commercial source. ICE recognizes that there are potential privacy risks and impacts on individual rights associated with the collection, use, and retention of LPR data. These include:

(1) LPR data in the aggregate may detail an individual's travel over time, leading to concerns about unwarranted surveillance.

(2) LPR data in the aggregate may provide details about an individual's private life, such as frequenting a place of worship or participating in protests and meetings, thereby implicating constitutionally-protected freedoms.

(3) A license plate image or read may be incomplete or inaccurate, because the license plate is bent, dirty, or damaged, or because the software or individual reading the numbers makes an error. This can result in the misidentification of a vehicle and its occupants.[5]

(4) LPR data may accurately identify the location of a vehicle, but it may not accurately identify the whereabouts of the person that ICE is seeking.

(5) LPR data may be accessed routinely, even when it is not needed.

(6) LPR data may be retained for periods longer than necessary for operational purposes.

(7) LPR data may be inappropriately shared with other agencies or private entities.

(8) New privacy risks and impacts on individual rights may arise as technological

[5] A recent case in California demonstrates that this concern is not just theoretical. *See* Green v. City of San Francisco, 751 F.3d 1039 (9th Cir. May 12, 2014).

advances create additional capabilities for LPR data collection and analysis.

ICE also recognizes, however, that there are clear benefits from the use of LPR data to both the ICE mission and the responsibilities of DHS overall. DHS privacy policies require that ICE assess the privacy risks in connection with the use of LPR technology and data, and follow the DHS Fair Information Practice Principles to the extent possible. DHS civil liberties policies support the evaluation of the risks to individual rights and liberties as a result of the use of LPR technology. These privacy and civil liberties risks and mitigating factors are discussed in detail below. DHS and ICE are committed to safeguarding PII, upholding civil liberties, and reducing potential risks posed by this technology.

Potential Impacts and Mitigating Safeguards

Data regarding a vehicle's location—particularly when collected over an extended period of time and retained—could potentially reveal additional information about an individual that is not necessarily used for a specific law enforcement activity or is sensitive because it reveals activities that might be constitutionally protected or that raise no law enforcement concerns.

Due to the growth in the availability of LPR data[6] and the potentially sensitive information it can reveal, ICE intends to implement a framework that will mitigate privacy and civil liberties concerns raised by the commercial acquisition and ICE's use, storage, and maintenance of LPR data. The requirements of the framework will be incorporated into any solicitation that ICE may issue for the acquisition of commercial LPR information, and will be documented in appropriate ICE policies. This framework will encompass:

1. Training – ICE will require all ICE personnel who are permitted to access LPR data via commercial subscription to first be trained on the nondiscriminatory use of the commercial system containing the LPR data and the agency's rules for acquiring and using the data, as described in this PIA. The vendor will be required to support the comparison of user lists against training records to ensure the training requirement is met for all users.

2. Specified Purpose – When logging into any commercial system that contains LPR data, ICE users will see a splash screen that describes the permissible uses of the system and requires a user to consent affirmatively to conduct only searches consistent with those uses. Among other rules for access, ICE personnel will be put on notice that an LPR read may not be the sole basis upon which an enforcement action is taken.

[6] One vendor estimates that it adds 70 million new license plates per month from private sources.

3. Timeframe for Query of Historical LPR Data – The privacy and civil liberties concerns associated with the retention of LPR data are exacerbated the longer the data is held by the vendor and made accessible for query. Operational necessity may require ICE to access information sufficient to establish patterns of criminal activity over time as part of an ongoing criminal investigation, or to identify the movement or location of priority aliens or known associates. The LPR framework will address timeframes for access to historical LPR records for both ERO and HSI, which require the data for different reasons and therefore need to query historical LPR data for different timeframes. For HSI criminal investigations, the limits on the authority to query historical LPR data held in the vendor database will be based on the applicable statute of limitations for the underlying crime that serves as the basis for the query. For ICE administrative investigations or enforcement actions conducted by ERO or HSI, the limit will be five years. ICE policy will allow exceptions to these time limitations if approved by a supervisor. ICE intends to require the selected commercial vendor to incorporate these use-based limitations into the query interface in the vendor system.

4. Use of an Alert List – ICE intends to require that the vendor provide the capability to store license plate queries in the form of an "alert list," whereby any new read of a plate on the alert list will result in notification to the ICE law enforcement officer who added it. This capability will assist in the identification of a vehicle's location in near real-time, which will contribute to law enforcement efforts to apprehend individuals whose location may be connected to the vehicle's location. While automatic notification that an individual subject is on the move could raise privacy and civil liberties concerns, such notification also serves an important law enforcement interest. To help reduce the potential intrusiveness of this technique, ICE policy will require that alert lists be updated once the enforcement matter is resolved, or the individual is no longer a subject of interest. Users will also receive training on the importance of promptly removing license plate numbers from alert lists to avoid gathering LPR data without adequate justification. The training will also encourage ICE personnel to reexamine their entire alert list on a regular basis, but at least annually.

5. Audit – ICE will require the vendor to provide for an audit trail of each query that is made, by whom it is made, and for what purpose. Specifically, the audit logs must capture the identity of the user initiating the query, the person for whom the query is initiated if different from the user, the license plate number used to query the LPR system, the date and time of the inquiry, the results of the user's query, the case or investigation number associated with the query, and the reasons for executing the

query. The audit trail should be generated electronically and will need to be available to and reviewed by ICE supervisory personnel quarterly or more frequently to ensure that the data is being used appropriately. In the event these requirements are cost prohibitive, ICE will work with the vendor to obtain information to establish a comparable in-house audit capability.

6. Accountability – ERO and HSI managers will be held accountable for ensuring that personnel with access to commercial LPR data sets are properly trained and use LPR data appropriately. Periodic reviews of audit logs will confirm this is occurring. The ICE Office of Professional Responsibility will investigate any anomalous activity uncovered in the audit logs and ICE management will impose appropriate disciplinary action.

Individual Rights and Liberties

ICE, in coordination with the DHS Chief Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties, has included in this PIA a discussion of civil liberties issues raised by the use of LPRs to more completely address public concerns regarding the use of this technology. The inclusion of an individual rights and liberties discussion in this PIA will improve transparency and assist the public understanding of ICE's use of LPR technology.

In addition to the above framework of privacy and civil liberties protections, existing DHS policies will foster the proper use of LPR data. DHS prohibits the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances. Accordingly, consistent with law and DHS policy, LPR data may not be collected, accessed, used, or retained to target or monitor an individual solely on the basis of actual or perceived race, ethnicity, or nationality. The following is the Department's official policy[7] on this issue:

> "Racial profiling" is the invidious use of race or ethnicity as a criterion in conducting stops, searches, and other law enforcement, investigation, or screening activities. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity. The Department of Homeland Security (DHS) has explicitly adopted the Department of Justice's "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," issued in

[7] Janet Napolitano, "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities" (Apr. 26, 2013).

> June 2003. It is the policy of DHS to prohibit the consideration of race or ethnicity in our daily law enforcement and screening activities in all but the most exceptional instances, as defined in the DOJ Guidance. DHS personnel may use race or ethnicity only when a compelling governmental interest is present, and only in a way narrowly tailored to meet that compelling interest. Of course, race- or ethnicity-based information that is specific to particular suspects or incidents, or ongoing criminal activities, schemes or enterprises, may be considered, as stated in the DOJ Guidance.
>
> Except as noted below, it is DHS policy, although not required by the Constitution, that tools, policies, directives, and rules in law enforcement and security settings that consider, as an investigative or screening criterion, an individual's simple connection to a particular country, by birth or citizenship, should be reserved for situations in which such consideration is based on an assessment of intelligence and risk, and in which alternatives do not meet security needs, and such consideration should remain in place only as long as necessary. These self-imposed limits, however, do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor.

ICE has adopted this policy and includes it in all manuals, policies, directives, and guidelines regarding any activity in which the use of race, ethnicity, or nationality may arise as a security screening, law enforcement, or investigative criterion. ICE personnel are trained on the policy.

Additionally, LPR data will only be collected and used in accordance with ICE Policy 10029.2 and future DHS and ICE policies governing enforcement actions at or focused on sensitive locations.[8] This policy is designed to ensure that enforcement actions do not occur at nor focus on sensitive locations such as schools and churches and public meeting spaces unless exigent circumstances exist, other law enforcement actions have led officers to a sensitive location, or prior approval is obtained. The policy is also meant to ensure that ICE officers and agents exercise sound judgment when enforcing federal law at or focused on sensitive locations and make substantial efforts to avoid unnecessarily alarming local communities. LPR data could support this policy by identifying alternate locations for arrest. The policy and other controls

[8] *See* ICE Policy No. 10029.2, Enforcement Actions at or Focused on Sensitive Locations (Oct. 24, 2011), *available at* http://www.ice.gov/doclib/ero-outreach/pdf/10029.2-policy.pdf.

will likewise help ensure that the use of LPR data does not have a chilling effect on free speech and association.

Finally, ICE will adhere to its investigatory policies and procedures, and to the greatest extent possible, verify the accuracy of vehicle information and any subsequent information obtained from other sources as a result of the LPR data. When LPR data is obtained during the course of an investigation or enforcement matter, ICE personnel will take into account the quality, integrity, and age of a given LPR record in assessing its value and use as an investigative lead. This requires human evaluation and verification to determine the relevance of LPR data to an active investigation or other authorized law enforcement or homeland security efforts. This also includes visually confirming that the plate characters generated by LPR correspond with the digital image of the license plate in question.

Fair Information Practice Principles (FIPPs)

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

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

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. As part of its law enforcement program, ICE uses LPR technology to conduct criminal investigations and civil immigration enforcement actions. As such, this PIA examines the privacy impact of LPR technology operations within the construct of the FIPPs.

1. Principle of Transparency

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

Privacy risk: There is a risk that individuals will not have adequate or meaningful notice that their license plate information will be collected by commercial license plate vendor services and shared with ICE.

Management strategy: ICE is providing detailed notice to the public about the LPR data it collects from commercial data sources primarily through the publication of this PIA and through the publication of an updated PIA before ICE begins using this enterprise-wide solution. ICE Privacy Act System of Record Notices (SORN) provide public notice of broad categories of information that ICE collects in connection with its mission-related activities. To the extent that LPR data is linked to an individual, it is encompassed in these broad categories of information.[9] In addition, the description of the commercial LPR data services ICE wishes to acquire will be published in appropriate federal procurement portals, such as FedBizOps, as required by law.

LPR data obtained in support of an ERO investigation or operation seeking to apprehend a priority alien for removal will be filed in recordkeeping systems, specifically the Enforcement Integrated Database, covered by the Immigration and Enforcement Operational Records (ENFORCE) SORN.[10] The ENFORCE SORN alerts the public that ICE collects "biographic, descriptive, historical and other identifying data" as well as "travel and other information." The SORN states that this information is gathered in support of "the identification and arrest of individuals who commit violations of Federal criminal laws enforced by DHS" and "the identification, apprehension and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens." The SORN also notifies the public that data is obtained from commercial and public sources, among other sources.

---

[9] As noted elsewhere in this PIA, ICE law enforcement personnel incorporate LPR data into existing agency law enforcement recordkeeping systems when such data is deemed relevant to ongoing criminal investigations or civil enforcement actions, such as immigration matters. Once incorporated into these recordkeeping systems, the data is covered by the SORNs applicable to those recordkeeping systems as described above. ICE SORNs can be found here: http://www.dhs.gov/system-records-notices-sorns.

[10] *See* DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE), 80 FR 11214 (Mar. 2, 2015).

LPR data obtained by HSI in support of an ongoing criminal investigation or investigation seeking to identify and arrest a priority alien who is amenable to removal from the United States, will be filed in HSI's case management system, which is covered by the External Investigations SORN.[11] That SORN notifies the public that records collected on subjects of investigations include "[l]icense information for owners and operators of vehicles" as well as "registration and license data," and "any other evidence in any form, including papers, photographs, electronic recordings, electronic data or video records that was obtained, seized, or otherwise lawfully acquired from any source during the course of the investigation." The SORN also notifies the public that data is obtained from commercial data aggregators, among other sources.

2. Principle of Individual Participation

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

Privacy risk: Individuals are unable to consent to the retention and use of their license plate data in a commercial database.

Management strategy: The existence of LPR cameras and the fact that commercial entities can record license plate numbers for law enforcement use is a matter that is the subject of increased attention in the media and elsewhere. Many areas of both public and private property have signage that alerts individuals that the area is under surveillance.

Allowing a fugitive or criminal alien, or an associated individual, to be involved in whether his or her LPR information should be accessed, collected, queried, or retained from a commercially-owned repository of LPR data would significantly interfere with and undermine ICE's law enforcement mission. For this reason, ICE does not seek consent for the collection or use of LPR data. As a general matter, ICE law enforcement records are exempt from the Privacy Act requirement that individual notice be provided for the collection of information.

[11] *See* DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).

3. Principle of Purpose Specification

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

LPR data may be accessed and retained by ICE when necessary to carry out its law enforcement missions under numerous authorities, including the Immigration and Nationality Act, various criminal and civil provisions in Titles 18, 19, 21, and 31 of the United States Code, and associated DHS regulations. ERO will use this technology and data in a manner consistent with its immigration enforcement priorities, which at the present time include criminal aliens, fugitive aliens, illegal re-entrants, and those individuals posing a public safety or national security risk. ERO as well as HSI, to the extent HSI is engaged in immigration enforcement activities, will only collect, use, and retain LPR data in furtherance of open cases, investigations, or ongoing enforcement actions and only when necessary based on a law enforcement need.

HSI will use commercial LPR data to identify leads for its ongoing criminal and civil investigations. HSI investigates a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States, such as: immigration crime, human rights violations, and human smuggling; smuggling of narcotics, weapons, and other types of contraband; and financial crimes, cybercrime, and export enforcement issues. HSI may query a commercial LPR database to identify the location and movements of investigative targets and associates in connection with its law enforcement activities. It may also use this data to track vehicles suspected of carrying contraband, such as smuggled goods. LPR data may be used to identify individuals suspected of involvement in illegal activity during the course of criminal investigations (surveillance use), and to locate wanted individuals and immigration targets, such as at-large criminal aliens, re-entry criminal targets, and immigration fugitives. The LPR data will be used in conjunction with other information to develop leads to further the investigation, including identifying new suspects and eliminating others from further consideration. This data will not be used as the sole basis upon which enforcement actions are taken.

4. Principle of Data Minimization

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

Privacy Risk: There is a risk that without appropriate controls and oversight, LPR data may be accessed routinely, even when it is not needed.

Management Strategy: This risk can be managed by preventing overcollection and retention of the information. ICE will implement internal policies and training emphasizing the requirement to query and use LPR data only when in support of a criminal investigation or to locate a priority alien. Audit trails will capture sufficient usage data to allow the identification of ICE personnel who do not comply with these policies. ICE employees will be required to review and validate each item on an alert list at least yearly; however, employees will be required to update the alert lists as needed when cases are resolved or when the location of a given vehicle is no longer of investigative value. The fact that ICE personnel will have to associate queries with cases or investigations in order to perform the queries will provide an enforcement mechanism for these requirements.

In addition, to ensure that LPR information is appropriately accessed, ICE will require that the vendor interface capture information about the query of a license plate number and link it to a specific ICE enforcement matter. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR technology or data. Any abuse or misuse of LPR technology or data will be reported and subject to disciplinary action, as appropriate.

Privacy Risk: Due to the availability of historical data in the commercial vendor databases, there is a risk that ICE may receive inaccurate, untimely, or irrelevant LPR data that is not consistent with the purpose for which the data is sought.

Management Strategy: ICE will impose limits on the time frame of an historical search of LPR data either by policy or by a limitation built into the vendor's query system. For HSI queries, the time limits will be tied to the statute of limitations applicable to the case giving rise to the LPR data. For ERO queries pertaining to a civil enforcement (immigration) matter, the time limits will be based on the average length of time for vehicle ownership, which is reported to be approximately five years.[12] The purpose of these limits is to allow ICE personnel seeking

[12] *See* Polk View (now IHS Automotive) auto industry marketing and forecasting (2012), *available at* http://www.autonews.com/assets/PDF/CA78146220.PDF (last retrieved on March 18, 2015).

to conduct a criminal investigation or locate a priority alien access to sufficient historical data to identify potentially viable leads, but not so long as to result in the unnecessary or excessive acquisition of information. In any event, ICE will not retain in its records the results of its queries of commercial databases unless the information is determined to be useful in connection with its legitimate law enforcement activities. These limitations and requirements will help to ensure ICE's access to and retention of LPR data are compatible with the purpose for which the data is sought and to minimize the risk of an over-collection of this data.

Privacy Risk: Without proper controls in place, LPR data may be retained longer than necessary for operational purposes.

Management Strategy: ICE policy will require that only LPR data that is considered relevant or useful to the investigation or law enforcement activity underway will be retained in ICE recordkeeping systems.[13] ICE personnel who have access to commercial LPR data will be trained on this requirement. The ICE law enforcement officer conducting the query will retain the subset of results he or she decides are relevant in the appropriate ICE investigative or immigration case file for the length of time prescribed by the applicable records schedule for that file. The full query results will be retained (i.e., saved) only for audit purposes and only in the vendor's IT system. Once the LPR data is incorporated into the ICE case file, it and other case file data may be queried and analyzed in other ICE systems established to perform analysis in order to generate additional investigative leads, such as locating targets and linking cases using location information. Retention of data in ICE criminal investigative files is governed by NARA-approved retention schedules, which provide for investigative case files to be retained for at least 20 years and sometimes longer depending on the nature of the case. Immigration enforcement case files are retained in the Enforcement Integrated Database for 75 years.

[13] Examples of such cases are those in which the location of specific vehicles or targets/associates suspected of operating those vehicles may be useful to bringing a law enforcement matter to a conclusion (e.g., closure of a criminal case, arrest of a priority alien).

5. Principle of Use Limitation

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

Privacy Risk: LPR data in the aggregate may detail an individual's travel over time, leading to concerns about unreasonable surveillance.

Management Strategy: As a matter of policy, and as reflected in this PIA and in the applicable Privacy Act SORNs that describe ICE's purposes for collecting data, ICE only retains license plate data linked or connected to a person of law enforcement interest or connected to a criminal activity.

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 ENFORCE), and pursuant to information sharing agreements that specify permissible uses of the data. ICE intends that the selected commercial vendor will construct an interface that will list ICE personnel rules for accessing the LPR database and ensure that an audit trail of queries is created. Part of this interface will be a banner or splash screen that ICE personnel see and must agree to each time they log into the system. The banner will specify various rules, including the permissible uses of the LPR data, a notice that no action can be taken solely on the basis of a query result, and that ICE's policy regarding sensitive locations may limit enforcement action when a read includes enough of the surrounding environment to raise concerns in this regard. In addition, ICE will contractually prohibit the vendor from using ICE's queries (the license plate numbers input into the system) for its commercial purposes.

6. Principle of Data Quality and Integrity

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

Privacy Risk: A license plate read sent to ICE may be incomplete or inaccurate because the license plate is bent, dirty, or damaged, or because the individual reading the numbers makes an error. This can result in the misidentification of a vehicle and its occupants.[14]

Management Strategy: ICE intends to use the services of a commercial vendor of LPR data that meets a high degree of accuracy in the dataset. Errors due to poor optical character

[14] *See* Green v. City of San Francisco, 751 F.3d 1039 (9th Cir. May 12, 2014).

recognition (OCR) of the photographed license plate number can result in mismatches between the license plate number queried and the results returned by the system. Data errors of this sort not only present risks to individual privacy, but also can waste ICE resources and delay the resolution of investigations or the apprehension of subjects. To reduce the risk that these errors will escape detection, ICE will require the vendor system to display in the results the actual picture of the license plate, so ICE users can visually verify if it is an accurate match. Use of the selected vendor's system over time will enable ICE to identify any significant issues with the system's OCR capabilities and unacceptably high error rates. At the outset, however, ICE will specify the OCR used by the vendor must meet a certain accuracy rate.

In addition, ICE personnel's ability to visually confirm a match will mitigate the risk that ICE will rely on erroneous vehicle location data in an enforcement matter. Another mitigating factor is that ICE personnel will be prohibited by policy from taking enforcement action predicated solely on LPR data. In any investigative matter, ICE personnel recognize that it is imperative that no action be taken unless the data is accurate, relevant, timely, and complete, to the extent possible. Checks of other databases will be performed to ensure that any action taken is based on the most current information available about the vehicle, location, and subject of the case. The potential for disciplinary action as well as legal liability will serve as an incentive to ensure that LPR information used during enforcement matters is accurate. Training will emphasize these requirements.

7. Principle of Security

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

Privacy Risk: LPR information collected by ICE from a commercial vendor may be inappropriately accessed or disseminated.

Management Strategy: One method for securing LPR data against unauthorized access or use is to limit the number of individuals who can access LPR databases, and ICE intends to ensure that only those who need LPR data for their mission-related purposes are able to query the commercial data source. Once an authorized query occurs, the LPR data deemed relevant to the case will be added to a case file in a record system (electronic or paper) that is secure.

The vendor will be required to maintain an immutable log of queries of the LPR data, and this log will be reviewed quarterly or more frequently by ICE supervisory personnel to ensure that LPR data has been accessed for authorized purposes only. Anomalies in the audit trail that reveal inappropriate activity will be referred to the ICE Office of Professional Responsibility for further action. ICE will ensure through contract requirements that any vendor supplying LPR

data to ICE employ data security technologies comparable to those required of ICE systems in order to protect the integrity of its data from hacking and other risks.

8. Principle of Accountability and Auditing

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

Privacy Risk: Commercial data is not subject to internal DHS auditing and accountability controls; therefore, there is a risk that these controls may not occur or be as robust as they would be if the system were internal to DHS.

Management Strategy:

Auditing

By contract, ICE will require the vendor to maintain robust audit trails and make them available to ICE for review. ICE will ensure that the commercial vendor records all transactions and queries of LPR data in immutable audit logs at the individual authorized-user level and that these logs are subject to review at any time. Specifically, system audit logs must capture the identity of the user initiating the query, the person for whom the query is initiated if different than the user, the license plate number used to query the LPR system, the date and time of the inquiry, the results of the user's query, the case or investigation number associated with the query, and the reasons for executing the query. In addition, the vendor interface will help capture information about the query of a license plate number that will link it to a specific ICE enforcement matter. This data will also be captured, thereby enhancing the usefulness of the audit trail data. If such functionality is not available, a local audit log will be kept by the ICE field office. Any vendor that supplies LPR data to ICE will need to demonstrate the capability to produce this log. The vendor will only be permitted to use the queries submitted by ICE to maintain the audit log. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of LPR technology or data. Any abuse or misuse of LPR technology or data will be reported and subject to disciplinary action, as appropriate.

Training

Before being granted access to a vendor's LPR data, authorized ICE users, contractors, and other law enforcement personnel must complete training that describes all of the above policy requirements and associated privacy, civil rights, and civil liberties safeguards. This will supplement existing mandatory training required of all ICE personnel on data security, data privacy, integrity awareness, and records management.

Conclusion

To carry out its mission effectively, ICE personnel need to be able to use multiple data sources. When there is an investigative need, commercial LPR data provides a useful piece of information to help locate the subjects of enforcement actions and investigations. ICE is mindful of the privacy and civil liberties implications of accessing commercial LPR data and intends to build constraints into any solicitation for LPR data services that will allow the use of this tool in ways that mitigate the privacy and civil liberties concerns. A significant mitigation is that ICE does not intend to create its own database of commercial LPR information but will only acquire data when there is a need for it to carry out its work. A further mitigation is that ICE will create a framework to guide its commercial LPR data acquisition that reflects policy constraints while permitting appropriate operational use of this tool.

Responsible Official

Daniel H. Ragsdale
Deputy Director
Immigration and Customs Enforcement

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security