December 27, 2017

Privacy Guidance: Agency Access to and Use of License Plate Reader Data and Technology

Direct questions about this guidance to the ICE Office of Information Governance and Privacy (202-732-3300).

I. Purpose and Applicability

As part of its criminal and civil law 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. License plate reader (LPR) data and technology provide an important tool to support ICE mission activities. To maximize the use of this tool consistent with privacy and civil liberties requirements, this document provides ICE personnel guidance on the acceptable use of LPR data and technology within the scope of their official duties. This document serves as interim guidance until the publication of an ICE directive.

II. Definitions

LPR Technology. A system consisting of a high-speed camera(s) and related equipment mounted on vehicles or in fixed locations that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device. The system automatically converts the digital photographic images of license plates and associated data into a computer-readable format, i.e., a "read," that contains LPR data.

LPR Data. Information derived from LPR technology, including but not limited to: (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.

LPR Database/System. Any central data repository that is used exclusively for the storage of recorded license plate numbers and other LPR data. The database/system may also use front-end tools that allow users to view and analyze data in different ways.

Commercial LPR Services. Query-based access to a LPR database offered by commercial vendors that provides some or all LPR data based on license plate numbers. LPR data is uploaded to the database from a variety of governmental and private sources including, but not limited to, access control systems, such as toll road or parking lot cameras; vehicle repossession companies; and law

[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.

enforcement agencies. Licenses to access commercial databases may be sold to commercial consumers as well as law enforcement agencies.

Hotlist. A list created by an ICE law enforcement officer in order to be automatically notified by an LPR database when a new "read" of a license plate associated with an ongoing investigation occurs.

III. ICE Uses of LPR Data and/or Technology

ICE will neither create and establish its own LPR database, nor contribute LPR data to any commercially-available LPR databases. ICE personnel may employ LPR data and technology only for authorized criminal and civil law enforcement purposes, including supporting criminal investigations into national security threats, illegal arms exports, financial crimes, commercial fraud, human trafficking, narcotics smuggling, child pornography and exploitation, and immigration fraud; identifying, arresting, and removing criminal aliens, fugitive aliens, illegal reentrants, and those individuals posing a public safety or national security risk; and enforcing other criminal or civil violations within ICE's enforcement mission. ICE personnel may use LPR data and technology in three ways, through: (1) ICE-owned LPR cameras, (2) cooperative arrangements with other law enforcement agencies (LEAs) or law enforcement task forces that collect LPR data and/or use LPR data or technology, and (3) commercial LPR services. These three uses are described below.

1. **ICE-owned LPR cameras.** ICE law enforcement personnel may deploy ICE-owned LPR cameras to conduct surveillance during criminal investigations. An LPR camera will be placed at locations relevant to a particular investigation. For example, ICE Homeland Security Investigations (HSI) may place a camera along a smuggling route or location outside a business where an investigative target is known to frequent.

2. **Other LEA or task force collection of LPR data or use of LPR technology.** ICE law enforcement personnel may gain access to LPR data through the establishment of cooperative arrangements with other LEAs or law enforcement task forces that collect LPR data and/or use LPR technology. All LPR data is collected solely by other LEAs and often put into a database to which LEA access is granted.

3. **Commercial LPR services.** ICE law enforcement personnel may obtain query-based access, using hotlists and license plate numbers, to commercially-available LPR databases maintained by commercial vendors.

Requirements surrounding the use of LPR data and/or technology differ depending upon which of the three uses ICE employs.

IV. Requirements for Use of LPR Data and/or Technology

General Requirements Applicable to All Uses of LPR Data and/or Technology. Requirements A – H apply to all three uses of LPR data and/or technology:

A. General Use.

1. ICE will access, collect, and/or use LPR data and technology only for authorized criminal and civil law enforcement purposes. Authorized law enforcement purposes mean that

ICE's use must be associated with an ongoing investigation, target of investigation, and/or targeted enforcement activity.

2. ICE will consider the quality, integrity, and age of a given license plate reading before using the LPR data in any case or investigation.
3. ICE will not take enforcement action based solely on data collected from government-run or commercially-available LPR databases. LPR data will be supplemented with other investigative information before enforcement action is taken.

B. Restriction on Over-collection. ICE will not engage in the over-collection of LPR data. ICE will limit its collection to appropriate timeframes, as described in Requirement J; limit its collection to vehicles, not individuals, as described in Requirement I; and, at this time, prohibit geographically-based queries of LPR databases where no license plate number of a target vehicle is known. This does not prohibit ICE's deployment of cameras in geographic areas of investigative significance to identify targets or investigative leads. ICE will not engage in the mass collection of LPR data in order to identify targets or investigative leads.

C. ICE Contribution to LPR Databases. ICE will neither build nor host any government-run or commercially-available LPR databases that store exclusively LPR data. In addition, ICE will not contribute LPR data to commercially-available LPR databases.

D. Sensitive Locations. ICE will access, collect, and use LPR data and technology in accordance with ICE Policy 10029.2[2] or any superseding policy on enforcement actions at sensitive locations.

E. Special Protections. ICE will not add license plate numbers to hotlists; or access, collect, or use LPR data and technology:

1. based solely on race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity, unless authorized by law and policy. [3]
2. solely for the purpose of monitoring activities protected by the U.S. Constitution, such as First Amendment-protected activity, unless authorized by law.

F. Data Storage. Storage devices associated with ICE-owned LPR cameras are to be stand-alone and not networked with any commercial databases or systems. LPR data from ICE-owned cameras may be transmitted back or uploaded to existing ICE systems [e.g., Video Evidence Collection and Distribution System (VECADS) or Investigative Case Management (ICM)] when it pertains to a target or targeted enforcement activity. After transmission or upload, the raw data will be deleted off the storage device associated with the ICE-owned LPR camera, unless it must be preserved on the device as original evidence and maintained by an ICE Evidence Custodian. LPR data collected from commercial or other LEA LPR databases may be uploaded to existing ICE systems (e.g., ICM) when it is found to be relevant to the investigation as a result of queries of those LPR systems.

G. Data Retention. ICE will not retain LPR data that is not related to the current ICE law enforcement investigation. Any data that is relevant to this investigation will be retained in

---

[2] See ICE Policy No. 10029.2, Enforcement Action at or Focused on Sensitive Locations (Oct. 24, 2011).
[3] See Department of Justice's Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (Dec. 2014).

the case file (e.g., ICM ROIs, Subject Records) to which the data pertains and not in an aggregated database.

H. Training. Before accessing commercial or other LEA LPR databases, ICE personnel will first be trained on the requirements for use to ensure compliance with this guidance. ICE personnel will also complete mandatory annual privacy and records training.

Specific Requirements Applicable to Commercial/LEA-Collected LPR Data and/or Technology. Requirements I – M apply specifically to ICE's use of commercial or other LEA/task force-collected LPR data and/or LPR technology:

I. Queries of LPR Databases. All queries of government-run and commercially-available LPR databases will be based on a license plate number queried by ICE law enforcement personnel. LPR data returned in response will be limited to matches of that license plate number only within the time period specified in the query.

J. Historical Queries. Depending on the type of investigation being conducted, ICE law enforcement personnel will query LPR databases for historical LPR data for only a certain period of time.

1. For criminal investigations, ICE will limit queries to the time period established in any statute of limitations for the underlying criminal violation.
2. For civil immigration matters, ICE will limit queries to the previous five years.

K. Hotlists.

1. All license plate numbers added to hotlists must be derived from and associated with current ICE law enforcement investigations.
2. Hotlists will contain only license plate numbers and any associated ICE-created tracking numbers. Hotlists will not contain any other identifying information about person(s) who may be associated with the license plate numbers.
3. ICE will document and maintain lists of all license plate numbers added to hotlists. Lists will detail at a minimum the license plate numbers, associated investigative case numbers, and any ICE-created tracking numbers. ICE will maintain these lists for five years after list creation date.
4. Hotlists are subject to review and refresh on at least an annual basis to ensure that license plate numbers no longer needed are removed. ICE personnel should make an effort to expeditiously remove license plate numbers that are no longer needed notwithstanding this annual review.

L. Analytical Tools. ICE may use analytical tools in LPR databases/systems to view and analyze LPR data to determine patterns and trends. For example, ICE may use analytical tools to determine the driving patterns and routes of travel of a suspect vehicle where a license plate number is known.

M. Auditing and Accountability.

1. When ICE personnel are accessing other LEA or commercial LPR databases, an audit log must be created that contains the following: (1) the identity of the ICE personnel conducting the query, (2) the license plate number entered as the query, (3) the data and time of the query, (4) the results of the query, (5) case or investigation number associated

with the query, and (6) the reasons for executing the query. Audit logs may be provided by the other LEA or commercial vendor. If not, ICE personnel must establish a method for manually tracking these items.

2. ICE personnel should review audit logs at least quarterly to ensure compliance with this guidance. Non-compliance, including inappropriate access and use, may be referred to the ICE Office of Professional Responsibility (OPR), when appropriate.

V. No Private Right of Action

This memorandum, which may be modified, rescinded, or superseded at any time without notice, is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the other lawful enforcement or litigative prerogatives of ICE.

Issued by: (b)(6) (b)(7)(C)

Lyn M. Rahilly
Assistant Director
Office of Information Governance and Privacy