MIDDLETON POLICE DEPARTMENT	DATE Nov 16, 2013	POLICY 15.1.05
SUBJECT: **License Plate Recognition (LPR) System**	REVIEWED June 14, 2019	*MRR*

History: 7/2013; 05/2015
WILEAG (5th Ed.) Standards: None

Contents

PURPOSE

A License Plate Reader (LPR) system is a computer–based system that utilizes special cameras attached to police squad cars to capture license plate information. The LPR system passively captures an infrared image of the license plates of moving or parked vehicles and converts them to a text file using Optical Character Recognition ("OCR") technology. The text is compared to various hot lists generated by various law enforcement agencies, including the National Crime Information Center ("NCIC"), Crime Information Bureau (CIB), Wisconsin Department of Transportation (WisDot), and the local agency, and generates an alert when there is a hit. The LPR system also transmits and stores the digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured to a shared MPSIS server. The stored LPR data can be queried by license plate number, time frame, and location and will return the reads (images of license plates and vehicles, date, time, and geographic coordinates) matching the search criteria. (Access and authorization to run queries is restricted to authorized police employees who have passed a background investigation, including CIB and FBI record checks by fingerprint identification.) Stored LPR data is not associated with and will not identify any person who is operating a vehicle. It only identifies a license plate number.

The LPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals

include providing information to officers that will assist in on-going criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, identification of individuals who pose a potential public safety risk to the community, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in our community through the identification and removal of stolen, and unregistered motor vehicles, the collection of overdue fines from parking scofflaws, and enforcement of certain regulations. In summary the LPR system will aid officers in ensuring the safety of our community.

The purpose of this policy is to provide members with guidelines on the proper use of Mobile License Plate Readers (LPR).

POLICY

It shall be the policy of this department that all members abide by the guidelines set forth herein when using LPR's to scan, detect, and identify vehicles or persons of interest, and when accessing and utilizing data captured from LPR's, thereby increasing the efficiency and effectiveness of its public safety efforts in a manner that safeguard the privacy concerns of law-abiding citizens.

DEFINITIONS

FOUO means For Official Use Only.

LPR means License Plate Recognition/License Plate Reader, sometimes referred to as ALPR (Automatic License Plate Recognition).

OCR means Optical Character Recognition

Read means a digital image of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR system.

Alert means visual and/or auditory notice that is triggered when the LPR system receives a potential "hit" on a license plate.

Hit means a read matched to a plate that has previously been registered on a "hot list" of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation.

Hot List means license plate numbers of interest to law enforcement agencies including, but not limited to, stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to "hot lists" circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. The Department of Transportation can provide lists of expired registration plates, and law enforcement agencies can interface their own, locally compiled hot lists to the LPR system. These lists serve an officer safety function as well as an investigatory purpose.

Stored LPR Data or Scanned File mean data obtained by an LPR of license plates that were read by the device, including potential images of the plate and vehicle on which it was displayed, and information regarding the location of the police squad car at the time of the LPR read.

PROCEDURE

Management

MPSISC has made available to member agencies a shared LPR server and system software. The MPSISC Administrator, at the direction of the MPSIS Commission, is responsible for maintenance of the MPSISC LPR server, data storage and security, system software, local agency administrator rights, automatic system upload of scanned data files to the shared server, and causing the regular updating of the WisDot LPR Hot Lists. The Administrator will at least annually provide LPR system status and usage information to the MPSIS Commission.

Participating agencies are responsible for procurement, installation and maintenance of cameras, local hardware, loading client software on to local machines, and system access and security. A local agency designated LPR Administrator is responsible for the functionality of local equipment, local user access control including on which machines the LPR software is installed, authorized users, passwords, user rights, and maintenance of local hot lists, local manually entered license plate numbers, LPR Stored Data Access Records (if any), and Secondary Dissemination Records. The local administrator shall periodically, at least annually, compile statistics of LPR uses and provide an update to the Chief of Police and Command Staff.

Local agency Chiefs shall ensure that the LPR system is operated in conformity with this policy and other department policies, procedures, rules and regulations, and report significant successes and policy violations to the MPSIS Commission. An audit shall be conducted by a person designated by the Chief of Police who is not the local administrator and shall determine the department's adherence to this policy and the procedures it establishes, as well as the maintenance and completeness of records contemplated by this policy. The Chief of Police will provide a report once per year to the appropriate local oversight Committee, Commission or Board accounting for the uses of the LPR System including any policy breaches and successes. The MPSIS Commission or local oversight body may sanction a local agency for significant breaches of this policy.

LPR data is confidential, for official use only (FOUO), and can be shared only for legitimate law enforcement purposes, or when required by law, a subpoena or court order, or unless such disclosure is required by the Rules of Court governing discovery in criminal matters. Dissemination to a non-law enforcement agency shall be approved by the Chief of Police. The local agency is responsible for making reproductions of stored scanned files and for placing a copy in the local evidence system. When LPR data is shared outside of MPSIS agencies, it should be documented in a local agency secondary dissemination record.

After the retention period, stored data shall be purged from the data storage device or system. The LPR data file retention period is 12 months, except in circumstances when the data is being used as evidence or for all felonies being investigated, or when required by court order or the law.

Authorized User Access

A. The use of the LPR system, equipment, or data is restricted to authorized police employees for official and legitimate law enforcement purposes. Unofficial, improper, or otherwise unauthorized use of the LPR system or equipment, or the unauthorized access, use, release and/or dissemination of LPR data will be considered a significant infraction of department policy.
B. A background investigation, including CIB and FBI record checks by fingerprint identification, must be conducted before an employee is authorized by the Chief to use or access the LPR system, equipment, or data.
C. Only employees who have been trained in its use and this policy may operate the LPR system or access stored LPR data.
D. Authorized police employees shall use their designated user identification and password when using the system.

Access to Stored LPR Data

A. Access to stored LPR data shall be limited to employees designated by the Chief of Police. These employees may be issued a unique individual log-in ID and passwords by the local administrator.
B. Employees needing to query stored LPR data, but who are not authorized, may request that an authorized employee make the query. For example, in some agencies dispatchers are authorized to access stored data.
C. Authorized employees may access stored LPR data upon a reasonable belief that the data may be related to or useful as part of a specific official action or investigation. Participating agencies should monitor the use of LPR data to prevent unauthorized use. Similarly, dissemination of stored LPR data outside of participating MPSIS agencies shall be documented in an LPR Secondary Dissemination Record. LPR data is for official law enforcement use only and any other dissemination shall be approved by the Chief of Police.

LPR Usage

A. At the start of each shift, users must log in using their designated user ID and password, enter their name or employee number in the location field, and ensure that the LPR system has been updated with the most current hot lists available. LPR operators may deselect hot lists to be monitored during their shift. Users should log out of the system at the end of their shift.
B. Trained and authorized officers operating LPR equipped squads should have the system in operation so as to maximize the opportunity to scan vehicles, compare them to the hot lists, and collect LPR data.
C. LPR's should only be utilized to record license plates that are exposed to public view (visible from public streets or from private property held open to the public), absent a court order.
D. LPR's or LPR data shall not be used to harass or intimidate any individual or group. It is a violation of this policy to use the LPR system or data because of a person's or group's protected characteristic, for personal use, or for the purpose or known effect of infringing upon First Amendment rights.
E. Employees should notify their supervisor of successful uses of the LPR system.

F. Any employee becoming aware of a possible violation of this policy, including but not limited to the unauthorized access, use, release and/or dissemination of LPR data, shall refer the matter to his or her supervisor.

Steps Preliminary to Police Action

Upon receiving a hit or alert, prior to initiation of a stop, the officer should:

A. Verify that the vehicle plate number matches the plate number run by the LPR system.
B. Verify the current status of the plate through dispatch or query. If the alert is valid, the officer should take appropriate action based on the type of alert. Officers are reminded that in some cases, the driver or occupant of the vehicle may not be the person with whom the license plate is associated. Officers should develop a reasonable belief that the operator or occupant is the person of interest (compare observed physical appearance with the physical description provided). If the officer remains unaware of any facts that would suggest that the owner is not driving, there is a reasonable assumption that the owner of a vehicle is the driver (State v. Newer).
C. Police actions or stops precipitated by an LPR alert will be documented using an incident or call number.
D. In any case, the officer may stop a vehicle where he/she has an independent reason for doing so, such as an unrelated traffic violation.
E. Nothing in this policy shall restrict or prohibit an officer from taking appropriate police action based on facts or reason obtained independently from LPR operation.

Hot Lists

The Department shall utilize hot lists that further the goals (supra) of the LPR system where there is a legitimate and specific law enforcement reason for locating a vehicle or a person. Legitimate and specific law enforcement reasons include, but are not limited to vehicles and persons reasonably suspected of being involved in the commission of a crime or public offense, persons who are the subject of an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list; vehicles with expired registrations; persons who are subject to a restraining order issued by a court, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and when information has been received concerning a specific individual or individuals who pose a potential public safety risk to the community.

Participating MPSIS agencies will utilize the following WisDot supplied hot lists.

Hot Lists	
Articles (Stolen)	License Plate (Stolen)
Boat (Stolen)	Local Agency Hot Lists
Canadian Stolen Vehicle	Missing Person
DOT Cancelled	National Sex Offender
DOT Expired	Probation

DOT History	Protection Order
DOT Restricted	Sex Offender
Foreign Fugitive	USSS Protected
Gun (Stolen)	Vehicles (Stolen)
Identity Theft	Violent Gang Member
Immigration Violator	Wanted Person

Local agency created hot lists and license plate numbers manually entered into the LPR system shall, consistent with this policy, be for a legitimate and specific law enforcement purpose.

Public Records Analysis Considerations

A. Requests for records are analyzed on a case by case basis to determine whether the record is exempt from disclosure under applicable law, or the public interest served by not making the record public clearly outweighed the public interest served by disclosure.
B. Requests for LPR records or data received by the MPSIS Administrator should be directed to the appropriate local agency or MPSIS Commission for analysis and response.
C. LPR data is confidential, for official use only (FOUO), and can be shared only for legitimate law enforcement purposes, or when required by law, a subpoena or court order, or when such disclosure is required by the Rules of Court governing discovery in criminal matters. Dissemination to a non-law enforcement agency shall be approved by the Chief of Police. Prior to disclosure pursuant to the Public Records Law or other requests outside of law enforcement, the Chief of Police shall consider all factors relevant to balancing the public interest in disclosure of a record against the public interest in non-disclosure including whether:
    1. Disclosure of LPR data would infringe on the personal privacy of individuals.
    2. Disclosure could affect the perceived character and reputation of an individual.
    3. Aggregated LPR data is uncorroborated and there may be errors in LPR reads of license plates.
    4. Disclosure of a person's location or pattern of travel could heighten the person's vulnerability to theft or physical harm.
    5. Disclosure would chill First Amendment rights by diminishing anonymity as the person travels to and from protected activities (protests, religious services, AA meetings, etc.).
    6. Disclosure of aggregated data could result in unsolicited contact of individuals by commercial enterprises.
    7. A record subject often has an enhanced right of access, however, in this instance this data is not associated with persons. Often a vehicle displaying a license plate is not used exclusively by one person or is registered to more than one person.
D. LPR System statistical information, secondary dissemination logs, stored file access logs, audits, and reports to oversight bodies, Commissions, or Committees may be subject to disclosure or partial disclosure.