ACLU
AMERICAN CIVIL LIBERTIES UNION
of OREGON

Testimony of Becky Straus, Legislative Director
In Support of SB 1522
Senate Committee on General Government, Consumer and Small Business Protection
February 10, 2014

Chair Shields and Members of the Committee:

Thank you for the opportunity to testify this morning in support of SB 1522, which would set out guidelines for the use of Automatic License Plate Reader surveillance technology by public agencies, including law enforcement.

This testimony is meant to repeat and also build upon the comments we delivered to this committee on January 16, 2014. Thank you again for your consideration of this important privacy and good-government issue and for your commitment to working with us to strengthen and improve the bill.

ALPR Surveillance Technology

Automatic license plate readers are cameras mounted on stationary objects (telephone poles, the underside of bridges, etc.) or on patrol cars. The cameras snap a photograph of every license plate that passes them by – capturing information on up to thousands of cars per minute. The devices convert each license plate number into machine-readable text and check them against agency-selected databases or manually-entered license plate numbers, providing an alert to a patrol officer whenever a match or "hit" appears.

When an automatic license plate reader system captures an image of a car, it also meta-tags each file with the GPS location and the time and date showing where and when the photograph was snapped. The system gathers this information on every car it comes in contact with, not simply those to which some flag or "hit" was attached.

As ALPRs become increasingly widespread, they are being put to a variety of uses. One of the most common law enforcement uses of license plate readers is to check plates against "hot lists," such as missing persons or outstanding warrant databases. Data collected from ALPRs can also be pooled in centralized databases. Software can be used to plot all of the plate reads associated with a particular vehicle to trace a person's past movements. The systems can also plot all vehicles at a particular location, such as the location where a crime – or a political protest – took place.

Additional uses for license plate readers are arising as the cameras become more affordable and widespread:

- Vehicle Verification: Photographs captured by ALPRs may contain more than simply the license plate, and sometimes include a substantial part of a vehicle, its occupants, and its immediate vicinity. Law enforcement can use captured photographs to verify witness descriptions of vehicles and confirm identifying features. Photographs of cars and drivers can also be printed and distributed to the press and public.
- Geofencing: Law enforcement or private companies can construct a virtual fence around a designated geographical area, to identify each vehicle entering that space. For example, in Tiburon, California, ALPRs monitor its only two roads that leave the town.
- Non-Law Enforcement: ALPRs can also be used for non-law enforcement purposes, such as repossession of vehicles and parking enforcement.

ALPR Surveillance Raises Privacy Concerns

When used in a narrow and carefully regulated way, automatic license plate readers can help police recover stolen cars and arrest people with outstanding warrants.

Unfortunately, automatic license plate readers are, for the most part, not being used in a narrow and carefully regulated way. The systems routinely store information on the location of innocent people. The scanning and storage capabilities of these cameras and data systems have grown exponentially since their introduction. And thanks to falling costs and the availability of federal grants, automatic license plate readers' ubiquity has also grown exponentially. Over time, these devices create a treasure trove of personal data – searchable logs tracking the movements of innocent Oregonians going about their private business. This technology can be used to track the movements of people who attend a protest or political event, attend a particular church, or visit a particular doctor.

Keeping track of suspected wrongdoers is one thing, but clear regulations must be put in place to keep authorities from tracking those who have done nothing wrong. State law should prohibit automatic license plate readers from storing or recording data after a reasonable period of time where there is no match to an offender list or other evidence of wrongdoing. Our laws should also guard against unwarranted disclosure of the data to third parties, to the public, or to any entity that does not share the same retention requirements as the entity that originally collected the data.

Roadmap for Smart Privacy Policies

The increased proliferation and advanced capability of surveillance technology raises issues not unique to ALPRs. Policymakers and members of the public should be asking a standard set of questions about all use of surveillance technology and these questions can then be a roadmap to the guidelines relating to license plate readers:

- **Usage.** What type of information is being collected and about whom? In what instances and with what limitations may the collection take place?

- **Sharing and Retention.** What happens to the data after it is collected? Can it be shared? How long is it kept?
- **Control.** Do individuals have the opportunity to know what information is collected about them and correct any inaccuracies?
- **Accountability.** Are there auditing mechanisms in place to ensure compliance with privacy policy and effectiveness of the data collection practices?
- **Transparency.** How can the public stay informed of usage and policy changes?

Lack of Consistency Regarding ALPR Policies in Oregon

In July of 2012 the ACLU of Oregon queried law enforcement agencies throughout the state to find out where ALPRs are and what policies, if any, govern their use. What we found is, of the handful of agencies that responded at that time, there is a clear lack of consistency regarding answers to the "privacy roadmap" questions we identify above. This inconsistency signals an urgent need to be thoughtful about how license plate reader surveillance can be applied in Oregon in a way that protects privacy.

Agency	Policy (Y/N)	Usage Restrictions	Sharing Restrictions	Retention Restrictions	Auditing
Medford PD	Y	"used only for official and legitimate law enforcement business"	Records Manager fills non-law enforcement requests "in accordance with applicable law"; Access to data for "legitimate law enforcement purposes only" (criminal, civil, or admin)	"Stored for minimum period established by department records retention guidelines, and thereafter may be purged unless it has become, or is reasonable to believe it will become, evidence…"	Training, authorized access; Login/password-protected system capable of documenting access
Oregon City PD	Y	Same as Medford			
Clackamas County Sheriff	Y	Plate data matched for information on stolen or wanted vehicles, AMBER Alerts, missing persons, warrant subjects, suspended drivers, uninsured vehicles, vehicles of interest, or "other user defined criteria"	"may be queried, accessed or disseminated, for official law enforcement investigative purposes only."	10 years	Training
Salem	N	"We load hot sheets			

Police		from California, Oregon, and Washington…. License plates of vehicles wanted for other reasons can also be entered." Also added City's "boot" parking records.			
Portland Police Bureau	Y	Attempt to avoid public gatherings (protests, etc.) unless there is a criminal nexus; law-enforcement purposes only	Access only with suspicion that data relates to criminal or civil action	Minimum 30 days, maximum 4 years. Can extent retention with reasonable belief	Training, annual report, login/password with access trail

SB 1522

Without any suspicion that an individual has committed a crime, ALPRs are used to search agency databases for his or her information. At the very least, clear policies and regulations must be put in place to prohibit storing or sharing data where there is no match to an offender list or evidence of wrongdoing.

SB 1522 proposes guidelines to enable use of ALPRs for public safety purposes and also protect the privacy of innocent Oregonians. The bill does not do anything to hinder uses of ALPRs that are laid out in current local law enforcement policies (listed above) and it provides additional benefit by putting forth sensible privacy protections in a way that will be implemented consistently across the state.

- Usage (Section 2)
    - Oregon Department of Transportation (ODOT) may use ALPR surveillance technology for regulating motor carriers and collecting tolls.
    - Law enforcement may use ALPR surveillance technology for enforcing parking and traffic violations and investigating crime.
    - Lists databases that ALPRs may be matched against: ODOT, National Crime Information Center (NCIC) of U.S. DOJ, Law Enforcement Data System (LEDS), state and federal missing persons lists.

- Sharing (Section 3)
    - Public bodies may share data with other public bodies so long as all parties comply with the retention requirements set out in the bill.
    - Public bodies may obtain data collected by private entities with a warrant.
    - Records are exempt from public record, except for a driver's own records. (Section 6)

- Retention (Section 3)
    - All data collected by law enforcement agencies may be kept for up to 14 days. After 14 days, the process for retention breaks into two categories:
        - "Hit" data: may be kept after the 14-day deadline if it is needed for an ongoing criminal investigation.
        - "Non-hit" data: may be kept pursuant to a court order based on reasonable suspicion that the data is relevant and material to an ongoing criminal investigation.

- Transparency (Section 4)
    - Agencies using ALPR surveillance technology must write and post on their website policies governing ALPR usage and post reports annually on how they are using them.

Amendments

After meeting with stakeholders including the Oregon Department of Transportation and law enforcement agencies, we have attempted to address concerns by drafting the following notable changes to SB 1522:

- Dash 1: ODOT amendments
    - Adds traffic research and analysis to the list of uses authorized for ODOT. Requires that data collected be de-identified so that it cannot be associated with an individual motorist.
    - Adds "tollway operator" to the list of authorized users of license plate readers when those tollway operators are using the readers for tollway enforcement. This provision is meant to allow for ODOT to contract with a private entity to conduct tolling operations.
- Dash 2
    - Amends prohibition on use of ALPR cameras that all might capture photos of individuals to say that any photos of individuals taken by ALPR cameras cannot be used.
    - Expands list of databases against which ALPR data can be matched to include out of state criminal justice databases.
    - Extends time period for retention of "non-hit" data from 14 days to 21 days.
    - Extends time period of court orders authorizing retention of ALPR data from 30 days to 180 days. Also permits court to grant additional time beyond 180 days upon a showing of "exceptional circumstances."
    - Clarifies that data retention restrictions apply to captured plate data and also to "any backup or copies of data."
    - Changes limitations on retention of "hit" data or data kept pursuant to a court order from conclusion of "criminal proceeding" to "resolution of criminal charges…"

We urge your support of SB 1522

The use of advanced surveillance technology is increasing at a rate much faster than our policies and statutes have kept up. Moreover, the public's awareness of this surveillance is minimal to none. Now is the time for this body to insert these modest privacy safeguards and transparency mechanisms into surveillance practices that are already in place. We urge your support of SB 1522.

Thank you again for your attention and consideration. Please do not hesitate to contact me at any time with questions.

Becky Straus
Legislative Director, ACLU of Oregon