

Summary List of EFF's State Legislative Agenda To End ALPR Mass Surveillance

The gold standard: lawmakers should ban police ALPR mass surveillance.

1. Ban state-level law enforcement agencies from acquiring, retaining, accessing, or using ALPRs or any data derived from them.
2. Ban local law enforcement agencies from doing the same.
3. Ban the use of state funds to acquire, maintain, or access police ALPR systems.
4. Ban installation or maintenance of police ALPRs on state-owned roads.

In the absence of a flat ban on ALPR mass surveillance, reduce its harms by limiting it to real-time comparison of passing plates to hotlists, and impose strict limits on the creation and use of those hotlists.

1. Limits on creating hotlists:
 - a. Limit the kinds of external hotlists that police agencies may link to.
 - b. Require a daily update of links to any external hotlists.
 - c. Forbid officers from adding a plate to a hotlist:
 - i. Absent a warrant;
 - ii. Absent a serious violent crime; and
 - iii. Based, in whole or part, on a person's race or similar characteristics, their First Amendment activity, or their pursuit of health care.
 - d. Require officers to log their entry of a plate on a hotlist, including the reasons.
2. Limits on using hotlists:
 - a. If a passing car's plate does not match a hotlist, require immediate deletion of all data about that car.
 - b. If there is a match, limit storage, search, and disclosure of the car's data to what is strictly needed for the investigation.
 - c. Require police, before stopping a car based on of an apparent match, to visually and independently confirm the match.

In the absence of a prohibition on storing ALPR data, reduce its harms by placing strict limits on police storage, search, and disclosure of ALPR data.

1. Storage limits:
 - a. Require deletion of ALPR data within days, not months.
 - b. Limit the types of ALPR data that may be stored: just photos of plates, computer-reads of plates, and the time and place.
2. Search limits:
 - a. Ban "geofence" searches of stored ALPR data for all plates in a particular time and place.

- b. Forbid officers from searching stored APRA data absent:
 - i. A warrant; and
 - ii. A serious violent crime.
 - c. Require officers to log their searches of stored ALPR data, including the reasons.
 3. Disclosure limits:
 - a. Ban disclosure of stored ALPR data to federal or out-of-state agencies.
 - b. Ban disclosure of stored ALPR data to another agency, absent its compliance with all of the search limits above.
 - c. Strictly limit an agency's participation in multi-agency disclosure networks like Flock and Vigilant.
 - d. Ban disclosure of stored ALPR data to investigate acts and statuses that are lawful in-state.
 - e. Ban any sale of stored ALPR data.

Ban three high-risk police ALPR practices:

1. Placement of ALPRs near sensitive locations like hospitals;
2. Purchase of ALPR data; and
3. Use of ALPR data to try to predict crime.

Require police transparency about their ALPRs, including:

1. A 30-day public notice before a city procures police ALPRs;
2. A statewide registry of all police ALPRs; and
3. Regular, independent, public audits, and statistical reports about police usage.

Ensure effective enforcement of all new ALPR restraints, including by means of:

1. A private right of action;
2. The exclusionary rule; and
3. Forbidding continued use of ALPRs by agencies and their contractors that recurringly violate the rules above.