Is your community considering Automated License Plate Readers (ALPRs)? Here's what you need to know:

ALPRs amount to dragnet surveillance. ALPRs capture license plate images without any suspicion of wrongdoing on millions of ordinary individuals. But a miniscule amount of that data is actually useful; the ACLU has estimated that less than 0.2% of plate scans are ever linked to vehicle registration issues or criminal activity.[1]

ALPR surveillance is revealing. Proponents of ALPRs claim that just collecting license plate information isn't a big deal. But ALPR data can reveal visits to the doctor's office, political demonstrations, and places of worship. Taken in aggregate, it can paint an intimate portrait of a driver's life—and can even chill First Amendment protected activity.[2]

ALPRs create a public records act nightmare. ALPR data is privacy-invasive—but must be public for transparency.[3] Some states have exempted ALPR data from their public records act laws because of privacy concerns, but the full extent of ALPR use is impossible for communities to understand without it, making ALPR data a dangerous transparency catch-22.

ALPR data retention is dangerous. ALPR data is susceptible to data breaches and misuse, but only a few states have legislation prescribing how long it can be kept—meaning it could be kept indefinitely. The longer ALPR data is retained, the more it reveals about the lives of drivers and the more chance it will be compromised or misused.

ALPRs can facilitate racial profiling. For example, in Oakland, lower-income neighborhoods are disproportionately captured by ALPR patrols.[4] In New York, ALPRs were used to target muslims. Mobile ALPRs "would drive down the street and record the plates of everyone parked near the mosque."[5]

ALPRs aren't always accurate. ALPRs can misread or misidentify plates. When that happens, the consequences can be serious. In 2009, San Francisco cops pulled over Denise Green, an African-American city worker driving her own car. At gunpoint, they handcuffed her, forced to her knees, and then searched both her and her car — all because an ALPR misread her plate and identified her car as stolen. Her experience led to a Ninth Circuit ruling that technology alone can't be the basis for such a stop. But that's not the law everywhere, meaning this kind of law enforcement abuse could happen in your community if ALPRs are adopted.

---

[1] ACLU, "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements" (July 2013) *available at* https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.
[2] International Association of Chiefs of Police, "Privacy impact assessment report for the utilization of license plate readers" (Sep 2009) at page 13, *available at* http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf
[3] Peter Bibring & Jennifer Lynch, "Los Angeles Cops Should Release Automatic License Plate Reader Records, EFF & ACLU Argue in Opening Brief" (Jan 28, 2015), https://www.eff.org/deeplinks/2014/01/los-angeles-cops-should-release-automatic-license-plate-reader-records-eff-aclu
[4] Jeremy Gillula & Dave Maass, "What You Can Learn from Oakland's Raw ALPR Data, Electronic Frontier Foundation" (Jan 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data
[5] Matt Apuzzo & Adam Goldman, "With cameras, informants, NYPD eyed mosques" (Feb. 23, 2012), http://www.ap.org/Content/AP-In-The-News/2012/Newark-mayor-seeks-probe-of-NYPD-Muslim-spying