What are ALPRs?

Automated License Plate Readers (ALPRs) are high speed cameras at intersections, along roadways, or mounted to patrol cars that track every car that passes its line of vision. AI software analyzes the photos to pick out characteristics of cars (like color, make, dents, bumper stickers, etc.) to create a searchable database. Police departments and private companies store and share this data — timestamped driving records of millions of people — for months and even years. The owner of this data is often the ALPR company.

ALPR technology can be used on any image from any camera from anywhere and invites the use of additional technologies, like facial recognition technology. The technology to read license plates, similar to the technology that can scan and "read a pdf, can be used on any image or footage taken by any camera. An OCR scan is not limited to any ALPR vendor's cameras. This opens a wide net and where, when, and how people can be surveilled.

ALPR Vendors

ALPR vendors are private, for-profit companies. Companies like Flock, Motorola, Axon, Verkada, Bosch, Rekor, and others who sell ALPRs profit from the perceived threat of crime and have no business interest in ending it. Their profit is driven by fear and the continuation of crime and violence in communities. As a result, the companies and their investors have no interest in creating a product that addresses the root causes of crime, conflict, and violence.

Motorola Solutions had revenue of $8.2B in 2021. Of that, $1.2B was sales of surveillance video hardware and software, including ALPRs. Motorola says its surveillance profit is growing by "double digits," and the majority of this growth comes from sales to law enforcement.

(Source: https://stocklight.com/stocks/us/nyse-msi/motorola-solutions/annual-reports/nyse-msi-2022-10K-22644777.pdf)

The business model of ALPR companies is to collect as much data as possible - not just ALPR data - and to share this data as widely as possible. Flock Safety built a product to sell to police that uses “people lookup tools, data brokers, and data breaches to "jump from LPR [license plate reader] to person," allowing police to much more easily identify and track the movements of specific people around the country without a warrant or court order." Flock boasts that its nationwide network collects 10 billion reads a month.

(Source: https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/)

All ALPRs are Dangerous

There is no way to effectively implement guardrails or firewalls in ALPR systems. The data is collected and it has been accessed by ICE for immigration purposes, by police to track protestors, and more.

ALPRs are dragnet surveillance which increase the power of police over criminalized communities, including black, brown, and poor people. Everyone is surveilled with ALPRs but a specific group of people are criminalized. ALPRs violate privacy but more importantly, they intensify police power.

A study of ALPRs in Piedmont, CA found that less than 0.3% of ALPR hits might translate into a useful investigative lead for police. Most of the license plates that were recorded were not on a hot list but police still have access to where people were at different times during their day. Flock Safety produces "transparency portals" aka a PR tool. From these tools, we can gather information on how many scans of license plates occur every month and the percentage of the scans that are "hits on the hot list." Generally, the reported data shows less than 1% of scans are for cars on the hot list meaning that ALPRs are dragnet surveillance and gathering data about everyone.

(Source: https://www.independent.org/news-release/2021/11/30/automated-license-plate-readers-a-study-in-failure/)

Other examples from outside the country of dragnet surveillance systems' data being open and available:

> "A massive Chinese database storing millions of faces and vehicle license plates was left exposed on the internet for months before it quietly disappeared in August." https://techcrunch.com/2022/08/30/china-database-face-recognition/
>
> https://www.thequardian.com/us-news/2022/oct/25/california-sherrifs-stop -black-drivers-five-times-more-white-people

ICE has contracted with data broker companies, like Thomson Reuters CLEAR program, to gain access to ALPR data from around the country. ICE has now amassed one of largest surveillance systems in the country through its acquisition of data via data brokers and partnerships with other law enforcement.

(Source: https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data)

In Illinois, county officials shared data criminalizing undocumented people with LexisNexis, which was then shared with ICE despite the City of Chicago passing a Sanctuary city ordinance.

ALPRs are routinely deployed in ways that reinforce racist policing practices. ALPRs can perpetuate the racist violence of policing. NYPD used ALPRs to monitor Muslims visiting mosques.

(Source: https://www.ap.org/media-center/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques)

This is about facial recognition, not ALPRs, but similar critiques stand and Tucson currently has cameras in public parks that capture biometric data. There is no outside accountability and little that can be done to ensure police follow any laws regulating their use of ALPRs and data. There are multiple examples of police from around the country ignoring laws intended to protect innocent people from surveillance by ALPRs. When there is little transparency, the police will violate the law. A police officer in Georgia was bribed to run a woman's license plate and a police officer in Ohio was using this technology to stalk their ex-girlfriend – these are regularly occurring events.

(More info: https://apnews.com/general-news-699236946e3140659fff8a2362e16f43)

ALPRs are machines and, like all machines, they make mistakes. This has led to dangerous encounters for community members who are mistakenly stopped by police when there is a faulty license plate read. There are many documented cases of ALPRs misreading license plates which have led to encounters where cops pull someone over and pull their gun on a driver of a vehicle that was mistakenly read to be on the hot list. Studies show that ALPRs misread license plates at least 10% of the time.

(Source: https://www.aclu.org/news/privacy-technology/san-francisco-woman-pulled-out-car-gunpoint-because; https://www.cbsnews.com/news/license-plate-readers-alpr-mistakes/; https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen)

There's no real mechanism for holding police accountable to which cars are added to hot lists.

(Source: https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and)