Massachusetts Should Facilitate – Not Inhibit – Law Enforcement Use of License Plate Data

ALPR Technology: Protecting Families, Communities, and Law Enforcement at the State and Local Levels

Ed Barron
Alan Slomowitz*

September 2013

* Ed Barron works on government relations matters at Greenberg Traurig, in their Washington, D.C., office. Ed served on three major committees over a 20-year span at the United States Senate. He was Deputy Chief Counsel for the U.S. Senate Judiciary Committee (for Chairman Leahy); Chief of Staff of the Senate Committee on Agriculture, Nutrition, and Forestry (for Chairman Leahy); and Deputy Chief of Staff of the Senate Environment and Public Works Committee (for Chairman Jeffords). In those capacities, Ed worked on a variety of legislative and legal issues over the years and received a special commendation for his "superior contributions to the law enforcement responsibilities of the U.S. Secret Service."

Alan Slomowitz focuses his practice on governmental affairs. He served 10 years as Chief of Staff to Representative Robert A. Borski (D-PA), senior member of the House Transportation and Infrastructure Committee. From 1989 until 1992, Alan also served on the staff of the Investigative and Oversight Subcommittee of the Public Works and Transportation Committee when Rep. Borski served as Chairman. His experience includes transportation infrastructure appropriations and legislation.

This research was supported by Digital Recognition Network and Vigilant Solutions.

Massachusetts Should Facilitate – Not Inhibit – Law Enforcement Use of License Plate Data

ALPR Technology: Protecting Families, Communities, and

Law Enforcement at the State and Local Levels

Automatic License Plate Recognition (ALPR) technology has been extremely effective in allowing law enforcement to use historical and real-time anonymous data to rescue or protect innocent citizens and capture criminals in thousands of cases without violating innocent citizens' privacy. ALPR technology allows law enforcement to rapidly scan thousands of license plates on moving or stationary vehicles and instantly compare the license plates against the FBI's National Criminal Information Center ("NCIC") database of license plates associated with active criminal investigations involving murder, rape, kidnapping, child molestation, child trafficking, terrorism, sex offenders, and missing persons. Combining historical and real-time data with FBI and other "hot lists" of license plates associated with terrorist or criminal activity allows investigators to quickly identify investigative leads.

A wide range of ALPR technology applications are in use today and are working well to save lives, solve and prevent crimes, protect critical infrastructure, recover assets such as stolen cars, and save law enforcement time and money. Private companies have greatly enhanced law enforcement efforts by providing access to ALPR data they have collected. Those companies generally work for financial institutions or insurance companies that are regulated by stringent privacy and compliance laws such as the federal Drivers Privacy Protection Act ("DPPA"). Their primary uses for ALPR data include repossession of vehicles for non-payment, recovery of stolen or lost vehicles, and fraud investigations. They have always employed private companies to take photos of license plates with hand-held cameras or to write down license plate numbers on paper to accomplish these objectives. ALPR simply makes these long-standing practices easier, cheaper, more effective, and more efficient to conduct, and the technology's growing use is a clear indication of its effectiveness.

A bill has been introduced in the Massachusetts State House that could greatly limit law enforcement access to anonymous ALPR data. H. 3068 (January 16, 2013) was introduced by State Representative Jonathan Hecht of Watertown and has been referred to the Joint Committee on Transportation. The bill would prohibit law enforcement agencies from retaining captured ALPR data for longer than 48 hours unless they obtain court approval. It would limit the ability of state and local law enforcement agencies to conduct investigations in which historical plate data may be of critical importance. Skilled investigators have used historical ALPR data to generate results in thousands of cases. Many of those results – on behalf of crime victims and their communities – would not have been possible under restrictions contemplated in H. 3068.

As it reviews the merits of ALPR, we strongly urge the General Court to take no action that has the unintended consequence of hindering law enforcement efforts or limiting lawful commerce. At issue is law enforcement's ability to quickly and cost effectively identify, pursue, and capture fugitives, rescue kidnapped or hijacked victims, respond to AMBER/Silver Alerts, monitor sex offenders, solve crimes, prevent attacks, and recover stolen vehicles. Also at issue is the ability of the private sector to use cutting

edge technology to become more efficient and effective at common tasks that have historically been completed manually.

The Massachusetts General Court should ensure the availability of ALPR technology and data for law enforcement and lawfully permitted commercial entities while safeguarding personal privacy. This paper describes ALPR technology, enumerates its benefits to public and private sector entities, describes existing privacy protections, and suggests how additional protections could be put in place without restricting the lawful use of the technology.

ALPR TECHNOLOGY HAS LED TO CRIMES BEING SOLVED THAT WOULD OTHERWISE HAVE GONE UNRESOLVED.

ALPR automates a process of that has been standard practice in law enforcement for decades. ALPR technology is an example of how to establish a good balance between privacy concerns and "big data" because the data is already anonymous. Personal information about the owner, passengers, or driver of a vehicle is not included on an actual license plate, and is not included in ALPR scans.

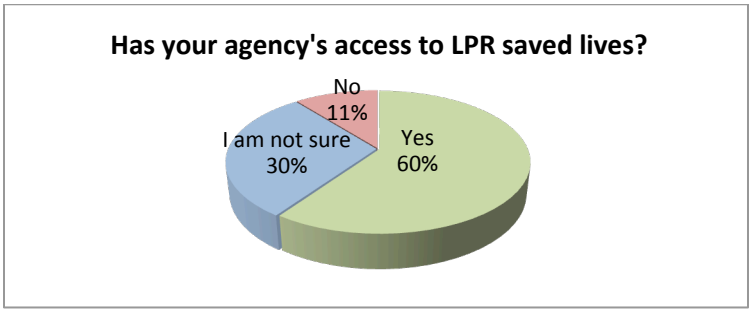
Throughout the nation there are thousands of real-life examples of how ALPR technology has protected families, communities, and law enforcement officers. Four examples are listed below.

(1) In the first 30 days of having access to a national ALPR data network that includes privately collected data, the Sheriff's Department of Sacramento County, California located 495 stolen vehicles, 5 carjacked vehicles, and 19 other felony vehicles (45 people were arrested).

(2) A 15 year-old girl was abducted in New York and taken to Maryland and repeatedly raped by her abductor. ALPR data led to the rescue of the victim and the suspect's capture and conviction.

(3) A mother reported her daughter missing after being unable to reach her for over a week. Detectives used ALPR data to identify the presence of the daughter's vehicle on three occasions in the prior week at an apartment complex. Working with property management, the detectives located the daughter, who was close to death.

(4) Police used an ALPR database to locate a fugitive responsible for identity theft crimes against ailing and deceased veterans. Around 50 victims reported charges on their credits cards entered with their names. All were from the same Veterans Affairs hospital in California. A suspect, who was an employee of the VA facility, fled to the Chicago area. Using the services of an ALPR provider, the police located the fugitive's vehicle in the Chicago area where she was arrested and later pled guilty to identify theft charges.



EXISTING LAWS – INCLUDING THE FEDERAL DRIVERS PRIVACY PROTECTION ACT – PROTECT CITIZEN PRIVACY AND GUIDE THE USE OF LICENSE PLATE DATA.

Federal law already protects citizen privacy with regard to license plate information. When some states began selling department of motor vehicles (DMV) information to marketers, Congress enacted the federal Drivers' Privacy Protection Act of 1994[†] to provide strong privacy protections regarding personally identifiable information held by state DMVs. The DPPA's purpose, as stated in the bill's preamble, was "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." More recently, the U.S. Supreme Court summarized the legislative history and explained that Congress decided to override state laws with the DPPA because of "the States' common practice of selling personal information to businesses engaged in direct marketing and solicitation." *Maracich v. Spears*, 570 U.S. (June 17, 2013). To protect privacy, the DPPA made "unlawful" any use of personal information obtained from motor vehicle offices (e.g., data taken from car registration or drivers' license applications) without consent unless it is for specific purposes authorized by the law such as for law enforcement; for any "private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions;" and for the execution of service of process or enforcement of judgments and orders pursuant to court orders; and for other purposes. (*See*, 18 U.S.C. 2721 – 2725).

Because of the protections put in place by the DPPA, the inability to connect license plate numbers to protected personal information held at DMVs without an expressed permissible purpose means that license plate numbers (whether obtained by writing them down, or by taking pictures manually or automatically with ALPR cameras) are anonymous data.[‡]

Note that the DPPA applies to <u>*any*</u> person – not just law enforcement – who misuses personal information and the DPPA applies to <u>*any*</u> person who makes a false representation to obtain any personal information from an individual's motor vehicle records. It is a very tough law in that actual harm (damages) does not need to be proven to get a judgment against persons who violate that law. *Kehoe v. Fidelity Federal Bank & Trust*, 421 F. 3d 1209 (11th Cir. 2005), *cert. denied*. DPPA provides for criminal fines for substantial noncompliance by State DMVs of not more than $5,000.00 per day of such noncompliance. Persons found in noncompliance are subject to civil action in U.S. district courts and may be ordered to pay actual damages, but not less than $2,500 in liquidated damages, reasonable attorneys' fees and litigation costs, and punitive damages, if justified.

As long as strong data privacy protections are in place, there should be no restriction on the ability of our protectors to take advantage of technology that helps them protect us. Privacy safeguards can be strengthened at the federal level with minor changes to the DPPA. At the state level, current DPPA provisions protecting the privacy of personal data held at the Massachusetts Registry of Motor Vehicles are sound. Measures recommended by some privacy advocates – including arbitrary time limits on how long anonymous ALPR data[§] can be stored – would clearly impair law enforcement's ability to identify

[†] The federal DPPA law was introduced in the Senate (S. 1589) in 1993 by Senator Barbara Boxer (with Senators Dianne Feinstein, Barbara Mikulski, Patty Murray, Tom Harkin and several other Senators). The House companion bill (H.R. 3365) was introduced by Congressman James Moran (with many cosponsors). President Clinton signed the bill as passed by the Congress.

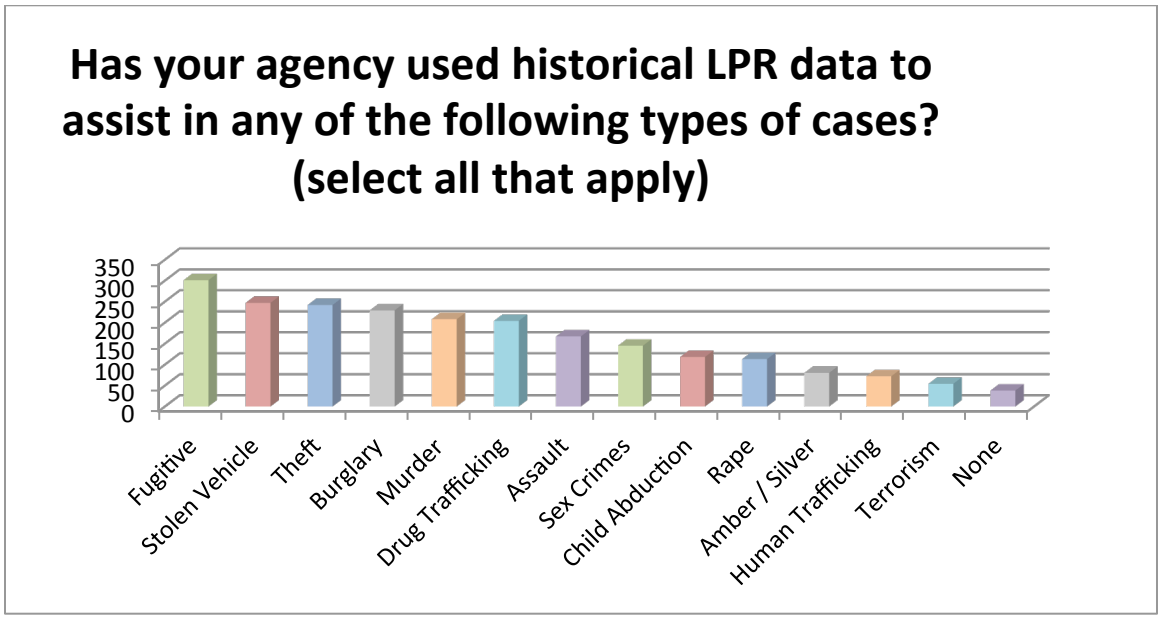
[‡] A few people pay extra for a "vanity plate" which could include their name.

[§] The use of historical data is very important regarding fighting organized crime and making longer-term associations regarding criminal gangs, drug trafficking organizations, and similar larger crime networks. In California, bank robbers took over a Wells

and rule out or exonerate criminal suspects, rescue victims, capture fugitives, prevent terrorist attacks, or arrest persons actively involved in crimes.

ALPR TECHNOLOGY HAS ENABLED MAJOR LAW ENFORCEMENT SUCCESSES NATIONWIDE, INCLUDING IN MASSACHUSETTS.

Many Massachusetts jurisdictions make use of ALPR technology. Supporting the search for suspects in the immediate aftermath of the Boston Bombing was just one example. Written testimony submitted to the Massachusetts Joint Committee on Transportation (May 16, 2013) quantified the tremendous public safety and economic impact generated by two ALPR technology companies over a five-year period.** In the short time preceding the testimony there were over 749,753 instances nationwide (538 in the Commonwealth of Massachusetts) where ALPR data – including historical data – provided by these companies was used by law enforcement to assist in criminal investigations involving murder, rape, kidnapping, child molestation, child trafficking, terrorism, sex offenders, assaults, and weapons related crimes. Those two companies provide access to their database *free of charge* to law enforcement officials upon request with over 30,000 investigators from over 3,000 law enforcement agencies using the system as of July 2013. To appreciate the importance of historical ALPR data in criminal investigations, consider survey responses from law enforcement users of ALPR technology in the graphic below.



Source: NetChoice survey of 506 law enforcement ALPR users conducted July 2013 - http://netchoice.org/library/research-2/netchoice-sponsored-survey-vigilant-solutions-law-enforcement-survey-on-license-plate-recognition/

While ALPR data use restrictions would clearly hamper interstate law enforcement efforts, States that create those restrictions may also violate the Takings Clause of the U.S. Constitution unless "just

---

Fargo bank but a witness got a license plate number as the suspects fled. A check of ALPR data showed the vehicle on a major highway six months earlier. Officers canvassed the area and quickly found the vehicle. They did a stake out and made the arrests.

** See Appendix G

compensation" is paid to the companies that created that valuable information. Electronically photographing license plate information is clearly lawful activity and protected by the First Amendment of the U.S. Constitution. Those anonymous photographs are valuable to many entities or persons including law enforcement, but also banks and insurance companies seeking to recover their property interests and detect fraud, or persons wanting to recover stolen cars. Under U.S. Supreme Court decisions, each State that imposes time limits on use of that anonymous data may have to pay just compensation if they force its destruction. Appendix E discusses two of the many U.S. Supreme Court decisions on this Fifth Amendment "takings" issue that could prove very expensive to states attempting to limit use of this valuable and lawfully obtained information.

THE AMERICAN CIVIL LIBERTIES UNION REPORT ON ALPR, TITLED "YOU ARE BEING TRACKED," MAKES SIGNIFICANT FALSE ASSERTIONS OF FACT AND LAW.

A recent ACLU "report"[††] criticizes ALPR technology on Constitutional privacy grounds. However, while their report is helpful in some respects, it is inaccurate and grossly misleading in other respects. The report makes a critical misstatement in suggesting that license plate data collected by ALPR is frequently "shared widely with few or no restrictions on how they can be used." That is simply not true. In addition to individual agency guidelines governing ALPR use, the federal Driver's Privacy Protection Act was designed by Congress to protect privacy rights with regard to license plate and other information. To the extent that ALPR allows law enforcement to save, protect, or rescue citizens, it also operates to protect each innocent citizen's right to life and liberty. Moreover, without access to official department of motor vehicle records, ALPR information is anonymous – it does not identify a specific person. Just like medical records are protected by law except for persons that are allowed to read them (physicians and other medical personnel), personal information held in motor vehicle departments, by federal law, is only available to law enforcement and persons working with law enforcement, matters related to motor vehicle or driver safety and theft, or recalls, the service of judicial process, insurance claims investigations, and other specifically authorized purposes.

In addition to existing legal protections, ALPR technology and data companies voluntarily impose strict requirements and limitations on the use of their data, and routinely monitor database access to prevent misuse or abuse. The combination of strong legal protections and industry's self-imposed data restrictions is why there has been no demonstrated pattern of ALPR data abuse anywhere in America.

The ACLU report incorrectly notes that ALPR is being "used to record Americans' movements" and thus "trace a person's past movements." There are two things wrong with this characterization. First, ALPR technology does not know who is driving or who is in the car. Second, it does not continuously trace all movements – it is not a continuous surveillance tool like GPS technology. ALPR technology only takes "snapshots" of a license plate (and the attached car) and notes the location, time, and date if a plate happens to be within view of a camera.

This is very different from GPS tracking technology, which is capable of tracing all of a vehicle's movements over time with high precision and involves physical trespass upon private property (a vehicle) in order to place a tracker. Because of these unique features of GPS technology, the Supreme Court in its 2012 *Jones* decision determined that GPS tracking constitutes a "search" under the Fourth Amendment and should be subject to a warrant requirement.

[††] "You are Being Tracked," July 2013, issued by the ACLU.

ALPR is also different from technology being promoted by the U.S. Department of Transportation that, over time, will monitor through wireless communications and other devices the relative movements of vehicles on a continuing basis. This new DOT movement monitoring technology is called Vehicle-to-Vehicle (V2V) or vehicle-to-infrastructure. It is labeled as collision avoidance technology and has already been tested by US DOT and when installed on a significant percentage of all cars in the U.S. it will keep relative track of moving locations of vehicles, speeds, where you stop, etc. DOT says it will "support a population of over 250 million vehicles using the system."[‡‡] In contrast, ALPR just takes snapshots of license plates that happen to be within camera view and notes the time and place.

The ACLU report also expressed concern that license plate numbers can be used by the police "to identify protest attendees merely because these individuals have exercised their First Amendment-protected right to free speech." The ACLU offered a helpful solution. They suggest that "only agents who have been trained in the departments' policies governing such databases should be permitted access, and departments should log access records pertaining to the databases." Fortunately, those practices are already in place thanks to requirements under the federal DPPA, requirements under individual agency policies, and strict requirements voluntarily imposed in contractual data use agreements between private ALPR data companies and their customers.

We also agree with the ACLU's position that taking photographs of things in plain view is a constitutionally protected activity. This includes license plates. As of August, 2013 the ACLU website notes that:

> "When in public spaces where you are lawfully present you have the right to photograph anything that is in plain view. That includes pictures of federal buildings, transportation facilities, and police."

This point is highlighted in ACLU legal briefs filed in court where they point out that the ACLU films and records audio of persons at demonstrations including the police because there is a "right to record information about the public activities of others."

The ACLU concludes that there is a "specific right to *record* information about the public activities of others . . . [including] recording 'street activities'." and there is a right to broadcast those movies of citizens, including police, in public places. The ACLU could then, "where appropriate," *broadcast* the recordings through "evolving internet and electronic media" such as through "Facebook, Twitter, and the ACLU's own 'action alert' email network'"[§§] They cite many cases for the proposition that "[c]ourts in myriad contexts protect the right to gather information for subsequent <u>public</u> dissemination." *See* e.g., *Richmond Newspaper v. Virginia*, 448 U.S. 555 (1980). (Emphasis added.) In contrast, the DPPA makes unlawful any dissemination of personal data including the photos and addresses of persons applying for driver's licenses except under very specific conditions.

One wildly misleading conclusion in the ACLU report is that the extremely small <u>*percentage*</u> of "hits" the police get for AMBER alerts, fugitives, criminals on the run, kidnappers, and other vehicle license plates associated criminal activity is evidence that ALPR is only of limited public safety utility. One need only talk to law enforcement investigators to find out the ACLU's conclusion ignores the reality of ALPR

[‡‡] For more details *see*: "Communications Security for a Connected Transportation Environment," US DOT, ITS Joint Program Office, Research and Innovative Technology Administration, FHWA JPO-11-130; "Fact Sheet: Improving Safety and Mobility Through Connected Vehicle Technology, U.S. DOT, National Highway Traffic Safety Administration; or TR News March-April 2013, "Keeping the Promise of Connected Vehicle Technology," or visit the ITS-JPO website, at www.its.dot.gov.

[§§] ACLU brief filed in *ACLU v. Anita Alvarez,* US Court of Appeals, 7th Cir; No. 11-1286 (Aug. 15, 2011), *see* especially pp. 12, 13 and 21.

usefulness to investigators. The hit rate is low because as compared to all vehicles, only a small percentage of vehicles are involved in crimes. That is a good thing. However, it is important to note that according to the International Association of Chiefs of Police, 75% of all crimes committed involve the use of a vehicle. Without ALPR technology, law enforcement has far less ability to find those needles in the haystacks.

LIMITING ACCESS TO ALPR DATA WILL RESULT IN DIRECT NEGATIVE FINANCIAL IMPACT FOR TAXPAYERS.

Costs are also a consideration, and an example from California highlights the potential impact. Leaving aside cases where seeking warrants would impede victim rescue and other efforts, consider that during a 12-month period from 2012-2013, California law enforcement agencies made approximately 60,000 queries to the private National Vehicle Location Service (NVLS) database. If those authorities had to get a warrant to access the same information, this would have cost roughly $300 to $500 in sworn officer and related staff and court time per request – that could mean $18 million to $30 million in hard costs.

It would also be cost-prohibitive for law enforcement to try to replicate the number of scans available for investigative queries through private sources. Technology acquisition and related costs would skyrocket for local and state agencies. Similarly, ALPR data retention limits would prevent the location of repeat parking offenders and essentially eliminate the collection of unpaid parking ticket revenues for state and local governments. It is estimated that the revenue that would be lost to local governments in California would be $54 million per year. From the resource perspective alone, ALPR enables great improvements in efficiency and effectiveness.

DELETING "OLD" ALPR DATA IS AKIN TO DELETING EVIDENCE THAT COULD BE USED TO APPREHEND CRIMINALS IN "COLD" CASES.

Time limits on ALPR data retention are unnecessary and counterproductive for two reasons. First, historical anonymous ALPR records do not, without being connected to DMV information, present a privacy threat. The federal DPPA protects that DMV information. Second, "old" ALPR data can be crucial to solving "cold" cases involving serious crimes. There are numerous examples where "old" ALPR records were used by law enforcement to solve major crimes. A recent survey conducted by NetChoice of law enforcement ALPR users yields dozens of cases. See: http://netchoice.org/library/research-2/netchoice-sponsored-survey-vigilant-solutions-law-enforcement-survey-on-license-plate-recognition/.

If the data is protected from unauthorized access, if frequent audits of system access are conducted, and if swift and significant penalties are in place to punish misuse, then the only meaningful impact of short data retention periods on ALPR would be to take potentially valuable investigative data out of the hands of law enforcement. Officers often cannot solve crimes without data placing perpetrators at locations where crimes had been committed. Historical data is a key in many investigations, and if it is deleted then a critical tool that is currently being used productively by officers and detectives around the country is gone. Police routinely store evidence of crimes – not associated with any person – for years. DNA samples not associated with any person (i.e., anonymous), but stored for years by the police can

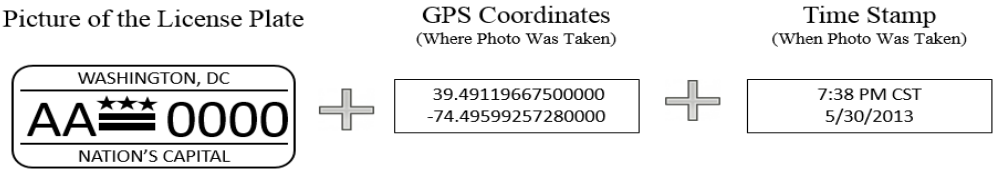
demonstrate the innocence of persons already convicted, or the guilt of the actual perpetrator, years later. Anonymous ALPR data – like anonymous DNA samples – should not be discarded, because just like DNA, ALPR data can help to exonerate or convict a citizen.

CONCLUSION

When examined through a factual lens and coupled with solid empirical evidence, no reason exists to legislate away or severely limit the use of ALPR technology or data. Thousands of citizens have been helped and thousands of criminals have been apprehended by law enforcement who were equipped with this life saving and justice serving technology. Simply put, ALPR technology is a highly effective tool for law enforcement tasked with protecting our communities.

APPENDIX A: What data does an ALPR camera collect?

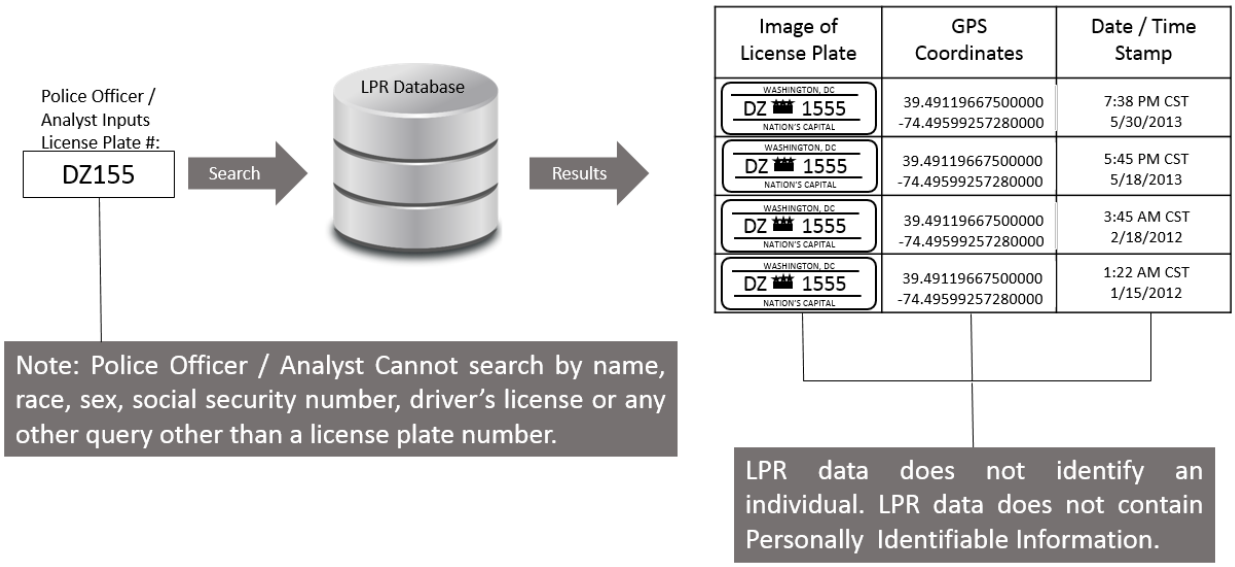
The data collected with ALPR technology does not identify an individual, does not include Personally Identifiable Information ("PII"), and therefore is by definition - anonymous data. ALPR cameras are only capable of collecting the following:



A picture and GPS location of a vehicle that is collected by ALPR technology is useless as a surveillance tool unless the user can associate an individual (i.e. the registered owner) with a specific ALPR record, or set of ALPR records for that vehicle. As discussed earlier, that is where the federal Drivers' Privacy Protection Act becomes crucial regarding privacy protections.

The data collected with ALPR technology does not identify an individual, does not contain PII, and therefore is by definition - anonymous data. It is not possible to invade the privacy rights of an individual by collecting or accessing anonymous data that does not identify an individual. ALPR data by itself is nothing more than a vehicle surveillance tool.[***] It can only tell you when and where a vehicle was photographed at a specific time or even numerous times. It is just as if you carried a GPS equipped camera in your pocket or use your GPS equipped smartphone to photograph cars including their license plates and used the photo date and time stamp function on the camera or smartphone. You could repeat this hundreds of times, if you had the time.

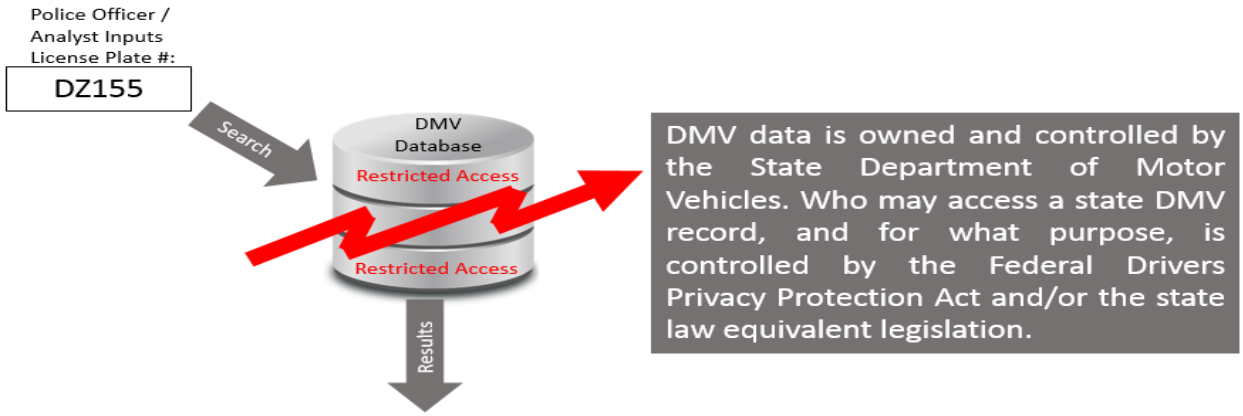
[***] ALPR technology is only capable of collecting the following data: i.) an image of a license plate; iii.) the date and time when the images were taken; and v.) the geographical positioning coordinates of the camera at the time the images were taken.



Photographs date and time stamps, and the GPS location(s) of a vehicle that is collected by ALPR technology is useless as a surveillance tool unless the police officer /analyst that has access to ALPR data can associate an individual (i.e. the registered owner) with a specific ALPR record, or a set of ALPR records for that vehicle.

APPENDIX B: Access to Department of Motor Vehicle data necessary to identify the registered owner of a vehicle is highly restricted.

It is possible to remove anonymity from an ALPR data record, but only if the user has access to a completely different database which is controlled by the Department of Motor Vehicles ("DMV"). Access to DMV data (Ex. name of registered owner, VIN, Year, Make, Model, address, telephone, etc.) is already strictly controlled by federal and state laws. State governments already have that data. That is where the second element of access minimization is instituted to create an architectural solution that provides the necessary oversight and limitation to protect against privacy abuse.



State Department of Motor Vehicle	
Vehicle Identification Number	XYZ1234THG8765P21
License Plate Number	DZ1555
Year, Make, and Model	2013 Ford F-250
Registered Owners Name	John Q. Public
Registration Address	123 Main Street, Anywhere, ST, 12345

As mentioned earlier in this analysis, whether it is for ALPR purposes, or for non-ALPR purposes, DMV access is already highly regulated by the federal Driver's Privacy Protection Act ("DPPA") and state law equivalents of the DPPA. Legislative limitations that minimize access to data are already in place to provide privacy protection in situations that do not involve ALPR data. A person may only access vehicle registration records under the permissible purposes defined by the DPPA or the applicable state law. In other words, strong state and federal laws already exist that extensively minimizes access to the DMV data separate and apart from ALPR data, but also applies and already requires compliance in order to utilize ALPR data as a surveillance tool.

For ALPR technology to reach its full potential, the current architectural solutions that protect privacy should be assessed particularly in the light of homeland security concerns and the increased risk of massive attacks such as bombings, release of poisonous gas, biological attacks, and the like. The residents of New York, Boston, Atlanta, Oklahoma City, Washington, D.C. and many other cities can attest to that.

APPENDIX C: General policy issues and recommendations

Apply DPPA privacy protections and disclosure requirements to ALPR data

To provide comprehensive uniform privacy protections while ensuring the viability of ALPR as a critically important law enforcement tool to prevent and solve crimes, and protect officers, families and communities, we recommend Congress enact federal legislation mandating that ALPR data shall have the same privacy protections and disclosure requirements as applies to data pertaining to drivers' license records as set forth in the federal Drivers Privacy Protection Act (DPPA) as amended (18 U.S.C. 2721-2755).

Uniform ALPR standards are needed to protect privacy and ensure that law enforcement authorities have the tools they need to prevent and solve crimes and protect public safety

Opponents of ALPR technology have framed legislation in several states that, if enacted, will severely limit its viability as a public safety and law enforcement tool, as well as its availability to the financial services and other industries with a legitimate and rightful interest in locating a particular vehicle.

For example, in 2012, SB 1330 was introduced in the California State Senate to ban the private sale or use of license plate recognition data. The bill required a search warrant for law enforcement use of such data. It also limited retention of private data to 60 days. Currently, private collection and use of LPR data allows law enforcement access to LPR data at no cost. If SB 1330 had been enacted, it would have eliminated private collection of ALPR data and severely limited its utility to law enforcement to prevent and solve crimes.

SB 1330's 60-day limitation on data retention would have prevented the solving of many crimes where past vehicle locations are key to identifying and apprehending suspects. It would also have prevented the efficient location of repeat parking offenders and essentially eliminated the collection of unpaid parking ticket revenues for state and local governments. This would have resulted in at least a $13 million reduction in state trial court fees from uncollected parking tickets per year.

The impact to local government public parking authorities is significantly greater. Using an average parking citation value of $50.00, the total amount collected by parking authorities in California was estimated to be $383 million annually. Based on a historical recovery rate of 14% using the ALPR technology, the revenue lost to local government from SB 1330 would have been $54 million per year.

As a result of these concerns, SB 1130 did not pass in in 2012. But if similar legislation is enacted in other states, this patchwork of state laws will effectively shut down private ALPR technology, denying local, state and federal authorities a critically important law enforcement and public safety tool that is vital to protecting the security of officers, families and communities. That is why Congress should consider legislation setting forth uniform ALPR privacy protections and disclosure requirements.

Appendix D: Examples demonstrating the value of ALPR technology

1) Crime: Methamphetamine possession, sales and possession of narcotics paraphernalia.

Outcome: Police used the NVLS database to pinpoint location of a male parolee who had multiple warrants at large. Suspect was captured with another parolee who had a stolen motorcycle in his possession. Two additional female suspects were also arrested for parole violations.

2) Crime: Homicide.

Outcome: Thousand Oaks Special Enforcement Unit used the NVLS database to determine a suspect's vehicle location in Oxnard. Location was the parents of the suspect's girlfriend. The investigators obtained the girlfriend's cell phone number, which led them to the successful arrest of the murder suspect 48 hours after the crime was committed.

3) Crime: Rape/sodomy/beating.

Outcome: LPR technology using the NVLS database was used to track the vehicle of a suspect to a Las Vegas apartment complex. US Marshals apprehended the suspect in the complex and he was taken into custody.

4) Crime: Home invasion where 68-year-old woman was held captive for several hours.

Outcome: Suspect fled the scene in victims car which was identified shortly thereafter in the NVLS database. Vehicle was found and the suspect was apprehended after a short foot pursuit.

5) Crime: Financial fraud with skimming machines, cloning devices and laptops.

Outcome: Police using the NVLS database were finally able to determine where suspects lived as a known vehicle was identified and traced to a large apartment complex in Anaheim. With the help of the United States Secret Service, multiple suspects were arrested.

6) Crime: Robbery, burglary and access card theft.

Outcome: A male suspect in multiple burglaries could not be found. It was determined his girlfriend had been driving him to some of the crimes and her license plate came up in the NVLS database resulting in the ultimate capture of both. The female was found guilty of committing other serious crimes.

7) Crime: Sex offender not living at registered address.

Outcome: San Jose Police used the NVLS database to locate the suspect's car on the other side of town and made a successful arrest. This and related parole violations resulted in a sentence of six years.

8) Crime: ID theft.

Outcome: The NVLS database was used to locate the suspect's vehicle in and around the Chicago, Illinois area. Within three days, US Marshals were able to find and arrest the suspect. She was extradited back to CA and recently pled guilty to multiple offenses.

9) Crime: Vehicle theft and vehicle burglaries.

Outcome: A neighborhood crime incident led neighbors to provide license plate information to the Riverside police who then used the NVLS database to determine that the vehicle was in a large apartment complex. The suspect was found and in possession of stolen property and arrested.

10) Crime: Commercial Burglary.

Outcome: A million dollars' worth of heavy equipment and rental tools had been stolen. The NVLS database was used to determine driving patterns of the suspect vehicle. These enabled police to monitor and apprehend a total of six suspects.

11) Crime: Racially related hate crime.

Outcome: ALPR data from the NVLS database was used to identify suspect's vehicle and ultimately apprehend him and a female who was an accomplice and witness to the hate crime.

12) Crime: Narcotics dealing.

Outcome: Sheriffs using the NVLS database were able to identify suspects car parked in front of a known gang house that had been linked to various crimes. This helped in surveillance leading to the seizure of several pounds of narcotics.

13) Crime: Strong-arm robbery.

Outcome: Culver City police using the NVLS database were able to identify the residence of two female suspects. They got a search warrant for the residence and were able to arrest the two gang members.

14) Crime: Identify theft of veterans.

Outcome: Police used ALPR database to locate a fugitive responsible for identify theft crimes against ailing and deceased veterans. Around 50 victims reported charges on their credits cards entered with their names. All were from the same Veterans Affairs hospital in California. A suspect, who was an employee of the VA facility fled to the Chicago area. Using the services of an ALPR provider, the police located the fugitive's vehicle in the Chicago area and she was arrested and pled guilty to the identify theft charges.

APPENDIX E: States could be financially liable for confiscating the value of anonymous ALPR data and could be required to pay "just compensation" to those who produced that information.

States that enact laws requiring that the ALPR data be "erased" within a certain time period may end up paying damages to the persons or companies that legally gathered or acquired that information. The U.S. Supreme Court has made clear that "intangible information" that has value is protected by the "Takings Clause" of the U.S. Constitution. The Clause prohibits the taking of private property for public use without just compensation. The Court noted that several factors are considered in determining whether a governmental action has gone beyond 'regulation' and creates a 'taking.' Among those factors are: "the character of the governmental action, its economic impact, and its interference with reasonable investment-backed expectations." *See Ruckelshaus v. Monsanto, 467 U.S. 986 (1984) and Sorrell Attorney General of Vermont v. IMS Health; 564 U.S. _____, (2011); 131 S.Ct. 2653 (2011)*

In *Sorrell v. Vermont*, a state law prohibited a commercial practice called "detailing," which related to data captured by private companies and used by pharmaceutical manufacturers to promote their drugs to doctors. Pharmacies receive "prescriber-identifying information" when processing prescriptions and sell the information to "data miners" who produce reports on prescriber behavior and sell or lease their reports to pharmaceutical manufacturers. "Detailers" employed by pharmaceutical manufacturers then use the reports to refine their marketing tactics and increase sales to doctors. Vermont's Prescription Confidentiality Law provided that, absent the prescriber's consent, prescriber-identifying information could not be sold by pharmacies and similar entities, or disclosed by those entities for marketing purposes, or used for marketing by pharmaceutical manufacturers. Vermont Stat. Ann., Tit. 18, §4631(d). The U.S. Supreme Court found that the First Amendment of the U.S. Constitution had been violated and struck down the Vermont law.

APPENDIX F: Sample results of a recent law enforcement survey

In a recent survey[†††] of 504 law enforcement officers who were asked about their use of ALPR information it was determined that:

76.1% - responded "Yes, without any doubt," to the question:

Do you believe that legislation prohibiting private companies from collecting, storing, and sharing LPR databases with law enforcement agencies would make it harder for you to investigate serious crimes and/or potentially result in serious harm or death to citizens within your community, your state, or the nation at large?

99.2% responded "no," to the question:

The July 2013 ACLU Report on LPR identifies potential misuse of LPR data for personal reasons other than official law enforcement purposes. Are you aware of any instance where you, a fellow officer, or anyone else has misused LPR data to track your boss, ex-wife, significant other, colleague, friends, enemies, neighbors, or family?

99.7% responded "no," to the question:

The July 2013 ACLU Report on License Plate Recognition identifies potential ways to misuse LPR data for political or profiling purposes rather than for official law enforcement purposes. Are you aware of any instance where you, a fellow officer, or anyone else has misused LPR data to target the owners of vehicles parked at political meetings, LGBT alternate lifestyle bars, gun stores, or abortion clinics?

One law enforcement officer provided special insight by noting:

"LPR is one of the important technologies for law enforcement investigative purposes in the past 40 to 50 years. I would put it up there with when law enforcement first started using cameras as a tool to document evidence. Or using computers to help their investigations, or using mobile data terminals, or even using a radio to be able to talk car to car or back to the station. It is an extremely important and effective law enforcement tool. The potential for misuse is so extremely low that the ACLU has no cause for concern whatsoever. There is virtually no way that it can be misused by law enforcement and if it is, that officer would be disciplined or terminated, again, making the potential so very low it is almost insignificant."

LPR data has become very valuable in locating, identifying and arresting serious and often times violent criminals. This information and the location of these individuals are extremely important to the arrest of these criminals and to the protection of the community at large. Limitations or prohibition of this information would be detrimental to the mission of public safety."

[†††] Survey conducted by Vigilant Solutions on behalf of NetChoice. Full survey data can be found at www.netchoice.org.