Information regarding Vigilant Solutions License Plate Reader system;

Automatic Number Plate Recognition (ANPR) was invented in 1976 at the Police Scientific Development Branch in the UK. However it did not become widely used until new developments in cheaper and easier to use software was pioneered during the 1990’s. The first arrest through detection of a stolen car was made in 1981 and the first documented case of ANPR in helping solve a murder occurred in November 2005.

During the 1990’s, significant advances in technology took automatic number plate recognition systems from limited expensive, hard to set up, fixed based applications to simple “point and shoot” mobile ones. This was made possible by the creation of software that ran on cheaper PC based, non-specialist hardware that also no longer needed to be given the pre-defined angles, direction, size and speed in which the plates would be passing the cameras field of view. Further scaled-down components at more cost-effective price points led to a record number of deployments by law enforcement agencies around the world. Smaller cameras with the ability to read license plates at higher speeds, along with smaller, more durable processors that fit in the trunks of police vehicles, allowed law enforcement officers to patrol daily with the benefit of license plate reading in real time, when they can interdict immediately.

Mobile ANPR, ALPR in the US, use is widespread among US law enforcement agencies at the city, county, state and Federal level. According to a 2012 report by the Police Executive Research Forum, approximately 71% of all US police departments utilize some form of ALPR. Mobile ALPR is utilized for recovery of stolen vehicles, monitoring for “Amber Alerts” and “Silver Alerts.” Recognized plates may be matched against databases including wanted person, (warrants) protections order, missing person, known and suspected terrorist and sex offender list.

There are a great deal of misleading statements and partial information being disseminated right now regarding license plate recognition, or LPR. This information claims that “Your are being Tracked” and that “LPR Invades your Privacy.” This is simply untrue.

Myth: You are being tracked.

Fact: LPR does not track. It is not ubiquitous. LPR captures point in time data on a vehicle, not a person.

Myth: LPR Invades Your Privacy

Fact: LPR doesn’t know who you are; it is anonymous data. A string of numbers and letters with a date, time, and location—that is all. It is only with a defined permissible purpose that law enforcement may “link” a license plate to an individual using another system to access DMV data. The act of making this “link” is governed by the Federal Driver’s Privacy Protection Act.
Myth: LPR can be used to see what political rallies and what church you attend, and can be used to determine patterns of what bars you visit, who you hang out with, etc.

Fact: the Federal Driver’s Privacy Protection Act already protects against this.

Questions:

What data is included in a license plate capture? Can officers see my medical history, social security number, or other personal data?

License plate captures include a color image of the vehicle, an infrared image of the license plate, the license plate read as interpreted by the system, a time and date stamp, GPS coordinates of the vehicle making the license plate capture, as well as information on the operator and the camera making the capture. In fact, only with permissible purpose under the Federal Driver’s Privacy Protection Act (DPPA) may an officer connect a license plate to an individual by accessing other systems. License plate reader data, by itself, is completely anonymous.

Is License Plate Recognition (LPR) considered tracking? Is a warrant needed?

LPR is unlike GPS devices, or other technologies that may be used to track. LPR is not ubiquitous, and only captures point in time information. And the point in time information is on a vehicle, not an individual. Individual drivers are already protected under the Federal Driver’s Privacy Protection Act. In the event that a vehicle becomes of interest in an investigation, it is still up to the officer to place a driver with the vehicle at the time of the crime. LPR data is an investigative lead only.

What about driver’s privacy?

License plate reader data, by itself, is completely anonymous; an LPR detection consists of a color image of the vehicle, an infrared image of the license plate, the license plate read as interpreted by the system, a time and date stamp, GPS coordinates of the vehicle making the license plate capture, as well as information on the operator of the LPR system and the camera making the capture. There is no personally identifiable information contained in a license plate capture. In fact, only with permissible purpose under the Federal Driver’s Privacy Protection Act may an officer connect a license plate to an individual by accessing other systems.

How secure is the Vigilant Solutions hosted server?

The Vigilant Solutions hosted server houses over 1.4 billion license plate reads, and grows at roughly 50 million reads each month, as of September 2013. This server and the services for hosting are managed
by Verio, a wholly owned subsidiary of NTT Communications, and a Microsoft Gold Certified Partner. Certified ISO 9001:2008 and compliant with SAS70 Type II, Verio is recognized as a world leader in hosted data and many Federal Agencies and Fortune 500 companies use the services of Verio. The data center itself is located just outside of Washington, DC, where Verio is headquartered. The data center itself features redundant power sources, redundant fiber connectivity, redundant disk arrays, environmental monitoring, secure access control, physical escorts for onsite visitors, multiple diesel fuel backup generators, active fire prevention and suppression, and onsite system administrators and engineers.

Due to sensitivities around LPR data, the entire network is secured by a Cisco router with firewall firmware compliant with PCI, HIPPAA, and SOX IT governance requirements. The Cisco firmware is also configured with Intrusion Protection Services offering deep packet inspection of all inbound traffic.

Is the solution scalable, and how can I guarantee uptime?

The solution is already capable of handling many more LPR systems and concurrent users than the present time (over 825 million reads and 25,000 users as of August 2012). The system is architected for almost infinite scalability under the management of Verio, and is guaranteed at greater than 99% uptime.

Who has access to the data on the hosted server?

Only credentialed law enforcement officers with a valid Originating Agency Identifier (ORI) number issued by the Criminal Justice Information System (CJIS) Division of the Federal Bureau of Investigation (FBI) may access the data on the hosted server. Access may be through the LEARN Back Office System for agencies using Vigilant’s ALPR systems, and/or via the National Vehicle Location System (NVLS) website which is open to any credentialed law enforcement officer.

Is it true that Vigilant Solutions has access to the NCIC database?

No. Vigilant Solutions LEARN Back Office provides the mechanism for an agency to use their own access to the NCIC database download, along with any other databases of interest.
License plate reader (LPR) technology has really come on strong during the last five years and the good news is that the technology keeps getting better, the prices have become more reasonable and the benefits of sharing the data have been recognized and acted upon by many agencies around the country.

Many articles have implied that LPR is an out-of-control, unregulated governmental intrusion on the private lives of ordinary citizens. The writers or quoted sources point to the millions of records on file, sometimes dating back two or three years and assert these records serve no legitimate public safety purpose. There is often a strong suggestion of potential abuse by unchecked governmental agents intent on prying into the lives of law abiding citizens with no history of wrong doing.

Although some have loudly criticized LPR as an unwarranted tracking of a private person’s everyday movements, LPR systems don’t really work that way.

Despite the efficiency of LPR and the millions of records that reside in many databases, an individual vehicle will only come to the attention of law enforcement in one or both of two situations: a) If the vehicle is on an alert or hot list (e.g. stolen or felony stop) at the time the license plate is initially captured (read). If this is the case, an officer generally takes whatever action is warranted. This is no different than an officer observing a vehicle and recognizing the plate from a hot sheet; b) When a query is made as a result of a criminal investigation and a vehicle or vehicles are identified as meriting follow-up. As an example, this could be the case when a crime victim reports a partial plate and an investigator queries the LPR database looking for the vehicle or vehicles with that plate combination that match the description provided by the victim.

Even with extensive LPR coverage, the LPR records are intermittent captures of encounters with vehicles and don’t come close to the full-time tracking of GPS devices.

Despite protestations to the contrary, LPR records are not personally identifying information, a legal term that assigns a greater level of scrutiny to data gathering. LPR cameras capture images of a vehicle and its plate, not the person who is operating it. The identity of a driver and his or her relationship to a vehicle to a vehicle is never assured because vehicles are instruments that can be shard and borrowed. Even the name of the vehicle’s registered owner is unknown to law enforcement without a separate query of a secure database that leaves an audit trail. This is significant because it essentially negates the concern that LPR is gathering extensive amounts of personally identifying information.

Although a single person may own a vehicle, this person isn’t identified in standard LPR operation and most LPR images don’t even display identifiable photos of the occupants. A great source of information is the International Association of Chiefs of Police (IACP) Privacy Impact Assessment (PIA) that was published in September, 2009. The electronic version of the document is available without charge at WWW.IACP.ORG, keyword LPR.

LPR technology is a powerful crime fighter and force multiplier. Not surprisingly, those who are opposed to LPR frequently and loudly proclaim that the technology could be misused. For instance, an officer could query the system to determine, for personal purposes, where a specific vehicle has been going.
In fact, the Wall Street Journal article on LPR cited an example of a Washington, D.C., police lieutenant using a law enforcement database to blackmail the owners of vehicles parked at a gay bar. Although the reference was used to make a point about potential abuse of LPR data, the actual case involved an officer using a vehicle registration database and had absolutely nothing to do with LPR. Further, the case points out that those who misuse databases are held accountable. In the D.C. case, the officer was fired and prosecuted for extortion.

Perhaps more relevant is none of the LPR critics have produced a single case of an LPR database being used for nefarious purposes. The reality: Other routinely used LE databases have much more intrusive and private information than an LPR system. For instance, a simple driver’s license check will tell you how much a person weighs, what their natural hair color is, when they were born, where they live and what their driving infractions have been. To suggest that LPR records should not be gathered because the resulting information might be misused is inaccurate.

ACLU

The ACLU published a report calling for restrictions on LPR technology because of potential misuse of the data.

The ACLU report used the word “risk” 12 times, “could” 7 times, and several “might” and “perhaps.” Much of the ACLU’s concern if over historical databases, where police and private companies are storing the date, time, and location of plates scanned by LPR cameras on police cars, along highways, or from private entities. The ACLU fears that historical LPR data might be “used by the police to track innocent people, or otherwise abused.”

The ACLU says little about how historical LPR databases help maintain public safety or recover vehicles.

Historical LPR data has helped to find criminals in thousands of cases, including those responsible for the failed Times Square bombing. One vendor has documented over 750,000 instances where their vehicle location data helped public safety officials in criminal investigations involving murder, rape, kidnapping, terrorism, assaults, and crimes involving children.

Another vendor allows LPR data access only to state-licensed professionals and contractors for regulated banks and insurance carriers. Since 2009 the vendor has helped recover over 190,000 vehicles worth over $1.3 billion that wasn’t passed along to car owners in the form of higher interest rates and insurance premiums.

The ACLU is worried that people might hack into these historical LPR databases to stalk or harass someone. But there are already laws against hacking, stalking, and harassment, regardless of the technology used.

The ACLU is also afraid because some “federal agencies illegally targeted activists in the civil rights, anti-war, and labor movements.” But this kind of discrimination is now illegal. Besides, LPR data is just a plate number, not the identity of the registered owner. To learn the owner, someone would have to
hack the Department of Motor Vehicles, which is a federal crime under the Drivers Privacy Protection Act.

Over the last few decades, some worried about the potential misuse of technologies such as Caller-ID and mobile phone cameras. Now, these are features we all expect. Instead of enacting new laws to ban these technologies, we enforced laws against bad behavior such as unlawful photographs, stalking, and harassment.