What's On Your (License) Plate?

Privacy Rights Versus Digital Driver Data Access, Creation and Accumulation of Driver Data by Law Enforcement

By John F. Breads, Jr.
Director of Legal Services
Local Government Insurance Trust

Local Government Insurance Trust
LGIT

LGIT's Legal Department

Staff of the Department of Legal Services include:

- **John F. Breads, Jr.,** Director of Legal Services - John oversees the operation and administration of the Legal Services Department.

- Attorneys - The department's attorneys defend LGIT members, their public officials, officers and employees in state and federal courts. They also assist LGIT staff and members with risk management issues.

    - **Christine T. Altemus, Senior Attorney**
    - **Matthew D. Peter, Senior Attorney**

Local Government Insurance Trust
LGIT

7225 Parkway Drive · Hanover, MD 21076 · Phone 443.561.1700
www.lgit.org

WHAT'S ON YOUR (LICENSE) PLATE?
THE RIGHT OF PRIVACY VERSUS LAW ENFORCEMENT ACCESS, CREATION AND ACCUMULATION OF DIGITAL DRIVER INFORMATION

"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." George Orwell, *1984*.

Introduction

In the futuristic, totalitarian society described by George Orwell in his novel *1984*, first published in 1948, every citizen was under constant surveillance by the authorities, mainly by telescreens. The people were constantly reminded of this by the phrase "Big Brother is watching you", the maxim on ubiquitous display. However, in the nature of doublethink, this phrase also meant that Big Brother was the benevolent protector of all citizens. Sixty-six years have passed since the publication of *1984*, and the year 1984 is thirty years behind us. From a technology perspective, the year 1984 seems like ancient history and what we now know makes Orwell's vision described so many years ago much closer to today's reality.

What we now know is that, in our modern world, digital and electromagnetic "fingerprints" are just as powerful identifiers as our own fingerprints. Directly or indirectly, from unseen up-close cameras to satellites far away, we can be, and often are being, watched. Ever-present computers, cell phones, smart phones, GPS systems, surveillance cameras, traffic cameras, body cameras, dash cams, and closed circuit monitors capture at least some trace of practically everything we do. This is not paranoia, it's fact. And the traces of our presence can be gathered, and potentially scrutinized, at any time and with virtually no chance that we will know that it is happening.

Just as the technology of the 80s has been long eclipsed, so has individual confidence in government to do the right thing. The recent disclosures concerning massive data accumulation by the NSA and other federal agencies have only added to the public's cynicism. Citizens are wary that secretly amassed information can easily be used against them – for whatever reason. And this concern is not just at the federal level. A recent editorial in Charlottesville's *Daily Progress* newspaper, said: "Secret information is an invitation to abuse. The time to set precedents to prevent such abuse is now, before problems become commonplace." And that battle as it pertains to mass data access and accumulation on private citizens – by all levels of government – is now underway.

The Exponential Growth of License Plate Reader Networks

Focusing on the state and local levels of government, we can begin with the widespread use by law enforcement of license plate reader ("LPR") networks. These digital networks use cameras mounted to traffic signals, road signs, and police cruisers to capture the movements of millions of vehicles in the United States. They do so by focusing on license plates, in which you have no expectation of privacy when they are publicly visible. The systems utilize LPRs, many of which are book-sized, to capture photo images that are translated into computer-readable text and compiled into an electronic list of plate numbers. The images capture the date, time, and location of the car. Police can then compare the license plate numbers against the license plates of stolen cars, of drivers wanted on

bench warrants, or even of persons involved in missing persons cases. Next time you pass a police car, know that the officer may be far more interested in you than it appears.

The last ten years have seen nothing short of explosive growth in the use of LPR Systems. Why? Cost aside (and the systems are far from cost prohibitive), the ever present threat of terrorism since 9/11 has resulted in technological advances undreamed of in 1984. From the federal government on down, law enforcement agencies are arming themselves, in many cases literally, with the tools and weapons to combat acts of terror, and not just to fight crime. In fact, the federal government, through the Department of Homeland Security ("DHS"), has fueled much of this growth. Many of LPR Systems in use by state and local governments today were funded by the DHS. Grants from the DHS are the primary funding arm for these networks. Beyond assistance to local governments, *The Washington Post* reported in February of this year that the DHS was seeking to have a private company provide a *national* license-plate tracking system – a system that would give the DHS access to vast amounts of information from commercial and law enforcement LPRs. The proposed "National License-Plate Recognition Database" would draw from license plate readers that scan the tags of every vehicle crossing their paths. According to the DHS solicitation, the system would help catch fugitive illegal immigrants. The proposal, however, failed to specify what – if any – privacy safeguards were to be put in place. And it is the lack of safeguards on such data that has fueled the debate. In this regard, the *Washington Post* article continued: "The [DHS] database could easily contain more than 1 billion records and could be shared with other law enforcement agencies, raising concerns that the movements or ordinary citizens who are under no criminal suspicion could be scrutinized."

The Beginning: The Driver's Privacy Protection Act (DPPA) of 1994

The concern over government and commercial access to personal information is nothing new. It's just that the ever expanding reach of technology results in intrusions that affect millions of people, and not just certain individuals. Literally unfettered access to driver information became a hot topic in the late 80s. In 1989, actress Rebecca Schaeffer was murdered by a stalker who had used a private investigator to obtain Schaeffer's home address from the California Department of Motor Vehicles. He subsequently went to her home and stabbed her to death at her front door. In the same time frame, pro-life advocates began to use public driving license databases to track down and harass abortion providers and patients. These happenings drew the attention of legislators who acted in response.

In 1994, Congress passed the Driver's Privacy Protection Act ("the DPPA"). This statute governs the privacy and disclosure of personal information (including photographs, Social Security numbers, names, addresses, telephone numbers, and medical or disability information) gathered by state Departments of Motor Vehicles. The statute was designed to limit Departments of Motor Vehicles, as well as other "authorized recipients of personal information," from disclosing it. Obviously, there were exceptions to the disclosure prohibition. Under the DPPA, information may be disclosed by a Department of Motor Vehicles ("DMV") (or re-disclosed by another entity, such as a police department), for any one of fourteen (14) exceptions, including: (1) for use by any government agency, including any court or law enforcement agency, in carrying out its functions; (2) for use in connection with matters of motor vehicle or driver safety and theft; or (3) for use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency, including service of process." Thus, during literally every traffic stop and/or vehicle impound, police officers will request that DMV data be accessed to determine license and registration status, owner identification, and other pertinent information including notifying owners of towed or impounded vehicles. Of importance, the DPPA also made it illegal to obtain drivers' information for unlawful purposes or to make false representations to obtain such information.

Abuse of the DPPA by Law Enforcement: The *Rasmusson* Case and Beyond

The DPPA was designed to, and has curbed many abuses of DMV maintained driver information. It can be argued, however, that when it came to law enforcement agencies, the statute remained unknown, or worse, ignored. A blatant example of law enforcement abuse of the DPPA came to light in 2009, when Anne Marie Rasmusson, then a police officer with the St. Paul (Minnesota) Police Department, learned from a fellow officer that he and his partner had used their squad car's computer to look up her driver's license photo. Under the DPPA, and departmental regulation, the DMV database was to be accessed only for police work. Officer Rasmusson was concerned and found that 104 officers in 18 different agencies across Minnesota had accessed her DMV photo record 425 times, for no legitimate law enforcement purpose. As reported in *Wired Insider* in 2012, an audit found that officers in the Dakota County Sheriff's Office and Bloomington Police Department, as well as state troopers, were among those who had illegally accessed Officer Rasmusson's DMV file over the course of nearly four years. Officer Rasmusson later left police work due to a work-related injury, but she also filed suit for the repeated violations of the DPPA (*Anne Marie Rasmusson v. City of Bloomington, et al*, Case No. 0:12-cv-00632 (U.S.D.C. Minn. 2012)). She contended that the activity involving her was merely a symptom of a larger problem involving data abuses by police generally. She also said that she feared retribution from officers for bringing the problem to light. In 2012, Rasmusson settled her lawsuit for more than a million dollars. In addition, over $130,000 in attorney's fees were awarded to Rasmusson's attorneys. One of the officers who was sued said: "I get [Officer Rasmusson's] side of it. But every single cop in the state has done this. Chiefs on down."

In another lawsuit in Minnesota, Beth McDonough, a local television producer and former crime reporter, is suing more than 40 governmental entities across the state over alleged snooping into her DMV driver's license file. As reported by Thomas Bullock in the Virginia Municipal League's *Law Enforcement Matters*, McDonough filed suit in federal court after learning that more than 170 law enforcement employees had viewed her DMV data nearly 500 times. McDonough alleges in her lawsuit that in 2007 or 2008, then Maple Grove police chief Mona Dohman told her: "People are fascinated by you. Be a little careful." Dohman, now the state's public safety commissioner, is one of the defendants.

Fear of lawsuits like the one brought by Officer Rasmusson has prompted many police agencies to begin to enforce the prohibitions of the DPPA. And the fear is not unfounded. Under the DPPA, plaintiffs can seek minimum damages of $2500 per occurrence, plus attorney's fees.

The DPPA and the Inclusion of DMV Information on Traffic and Parking Tickets and Citations: The *Senne* Case

The *Rasmusson* case shed light on the *abuse* by law enforcement officers of the DPPA. But, just as recently, another potential for liability under the DPPA was exposed – this time not from abuse, but from merely incorporating information from DMV databases on police tickets, citations, and other charging documents and reports. In 2010, Jason Senne, a resident of Palatine, Illinois, was issued a parking ticket. The ticket was left on the windshield of his illegally parked vehicle. Senne found the ticket the following morning and noticed that it contained a lot of personal information – including his name, date of birth, height and weight, address, and driver's license number. The ticket also listed for Senne an address other than the one where he resided. The address was his mother's address. Senne properly surmised that the issuing officer had obtained the information from the DMV, and felt that this alone was a violation of the DPPA. About one week after receiving the ticket, Senne filed suit in the United States District Court for the Northern District of Illinois (*Jason Senne v. Village of Palatine*, Case No. 10 C 5434 (N.D. Ill. 2010)). He sought and obtained certification of the case as a

class action on behalf of each and every individual who received a parking citation in the Village of Palatine during the previous four years if the citation included the individual's personal information. The Village moved to dismiss the suit on grounds that the DPPA did not apply to its placement of personal information on parking tickets, because the placement fell under one of the "permissible uses" (law enforcement) outlined in the statute. The Village also argued that the information was not "disclosed" because the ticket was left face down under Senne's wiper blade. The court agreed and granted the Village's motion. Senne appealed.

The appellate court disagreed with the trial court, ruling that the placement of the personal DMV information on the ticket was, in fact, a disclosure under the DPPA. The court said it didn't matter that the ticket was left face down. The simple act of placing a ticket face down on a windshield, rather than face up, is still a publication of the information and does not render it unavailable to the public. However, the appellate court sent the case back to the federal trial court to determine if the Village actually used the disclosed DMV information for its stated "law enforcement purpose." In doing so, however, the court expressed its skepticism: "With respect to some of that information [on Senne's ticket], it is difficult to conceive, even on a theoretical level, how such information could play a role in the excepted law enforcement purpose."

Upon return of the case to the federal trial court, the Village provided evidence that the DMV information disclosed on the ticket was actually used for a variety of purposes allowed under the DPPA. Specifically, the Village, through its chief of police, urged that there were more than a dozen law enforcement purposes for including the personal DMV information on parking tickets. Only a few, however, justified, in the eyes of the court, the inclusion of the information on the ticket. These included: (1) the fact that watch commanders at police stations used the ticket information to consider whether to void tickets claimed to have been erroneously issued to out-of-towners; (2) the fact that personal information on tickets served the same identification purpose during traffic stops in which the driver had no identification but did have a parking ticket in his possession; (3) and the fact that the personal information on the tickets helped drivers when an officer issued a ticket to the wrong person. Senne argued in response that the envelope copy of the ticket being left on a car is to inform the vehicle's operator that they have violated an ordinance and that the vehicle owner may be financially indebted to the Village. He argued further that the officer who issued his ticket did not need or use the personal information for anything and that held true for the clerks in the finance department who processed payments – by using the ticket number only, not any personal information on it.

With the evidence before it, the court was left to decide this critical issue: How does a court go about determining whether the disclosed information *is actually used* for the purpose stated in the DPPA's exceptions? Does a court do so on a case-by-case basis, to see if the use in a given situation was warranted – or is a general policy justifying the use enough? Does the DPPA require proof that the information is always used for the identified purpose? Is it enough that it *sometimes* is used for that purpose? Or is the possibility of use for the particular purpose sufficient? Further, does the party claimed to have disclosed personal information have to establish that a permissible purpose motivated the disclosure in the first place, or is an after-the-fact justification or an incidental use sufficient? In November 2013, the federal trial court in the *Senne* case concluded that the correct reading of the DPPA is that the *ultimate or potential use* of personal information qualifies as an acceptable use under the DPPA if it is for a permissible purpose such as law enforcement. Thus, the court held that even though officers may not use the personal information acquired from the DMV as to each ticket issued, just the potential that the information could be used in the future for a legitimate, law enforcement related purpose was enough to satisfy the DPPA. In other words, the DPPA contains no requirement for immediate use of the information. Based upon this holding, the trial court dismissed the case. Needless to say, Senne has again appealed.

The ultimate outcome in the *Senne* case has a lot of State and local officials worried and for good reason. As reported in October 2013 in the *Greenfield (Wisconsin) Patch*, the local chief of police there said, "[t]hey're calling (Senne's) ticket the $78 million parking ticket because (Senne's) attorney believes the city should pay $2500 for every ticket they've issued." That's $2500 for each of the 32,000 parking tickets issued by Palatine over a period of four years. LGIT will monitor the progress of the case in which no decision is expected until sometime late in 2015.

The New Frontier: License Plate Reader Networks

The DPPA is designed to prevent unauthorized access, including unauthorized access by police, to personal information stored in DMV databases. High-tech LPRs, on the other hand, are used to create *police databases*. The LPR scans registration plates to check whether drivers have outstanding parking tickets, lapsed registrations, lapsed insurance, or other violations. The LPR records the time and place registration plates are scanned – and alarms are tripped if violations are detected – and problems are solved. That certainly seems harmless enough. But is it? In late 2013, the Boston Police Department inadvertently released to *The Boston Globe* newspaper the license plate numbers of more 68,000 vehicles that had tripped alarms on LPRs over a six-month period. As reported in *The Boston Globe*, many of the vehicles were scanned dozens of times in that period alone. A public records request for the scan data was made in January 2013. The police department at first balked at the request, but then agreed to provide a database of license plates that had triggered alarms, but without the individual plate numbers. The information released, however, not only revealed full plate numbers, but also location data for more than 40,000 vehicles, most of which belonged to private citizens. To its credit, the newspaper discovered the error and did not publish any individual plate information. In response to the release of the unredacted information, the Boston Police Department indefinitely promptly suspended its use of high-tech LPRs.

The inadvertent release of information raised concerns not only about whether the police can reliably protect the sensitive data they collect, but whether police were actually using or following up on the scans at all. As stated above, the released information showed that numerous license plates had repeatedly tripped alarms for the same offenses, seemingly without any police action. The suspension of the scanning program did not appease privacy advocates. To the contrary, they continue to argue that the breach shows just how easily the technology itself can be misused. The advocates, including the ACLU of Massachusetts, ask if law enforcement could be trusted to police itself when it comes to this type of information. The problem, many argue, is in the proliferation of LPR use itself. The more LPRs, the more information, and the more information, the greater the potential for abuse. The LPR system used by the Boston Police Department enabled it to scan as many as four million vehicles a year. Although the department *had a written privacy policy* regarding the information gleaned from LPRs, the LPR program had never been audited to see the policy was working. Privacy advocates contend that the inadvertent release of the information to *The Boston Globe* shows that at least in one glaring instance, it was not. Beyond privacy issues, one ACLU official said: "You can't help but wonder whether the real purpose (of the scanning project) is simply to collect droves of data about where innocent people are driving, in case it might be useful for investigations later."

One component of the information gathered by LPR networks is generally overlooked. That is the ability of such networks to capture a vehicle's movements. LPRs can tell a police officer not only if your registration is expired but exactly where your vehicle was when this fact was discovered. In response to the broad sweep of information captured by LPRs, including vehicle location, local lawmakers have created a patchwork of laws and regulations trying to control the use of the information stored in LPR databases. For example, in Boston, in response to the breach of privacy caused by the Boston Police Department, Jonathan Hecht, a State (Commonwealth) representative,

proposed a bill to regulate the use of LPRs and the data they collect. As reported in *The Boston Globe*, "Hecht's 'License Plate Privacy Act" would slash the plate retention period to 48 hours except by court order and require [police] agencies to report annually on their scanner use."

Such local legislation, however, is not enough to appease privacy and civil liberties advocates. They want to fight this battle at the federal level. When interviewed recently by Tami Abdollah of the Associated Press (as reported by KIRO TV in Los Angeles), Michael Robertson, a tech entrepreneur fighting in court *to access LPR files for his own car*, said: "If I'm not being investigated for a crime, there shouldn't be a secret police file on me" that details "where I go, where I shop, where I visit." That's crazy, Nazi police-type stuff."

Robertson's case, filed in San Diego against the San Diego Association of Governments, has thus far been unsuccessful. San Diego Superior Court Judge Katherine Bacal has tentatively ruled that the local police agency (which keeps scanned data for up to two years) can deny Robertson's request for scans on his own vehicle under California's open records law because the information pertains to police "investigations." The judge has entertained further arguments and intends to issue her final decision soon. Robertson said he will appeal if he loses. In the same article, The Associated Press also reported that a petition by the ACLU of Southern California and the Electronic Frontier Foundation to access one week of scans on all vehicles collected by the Los Angeles Police Department and the Los Angeles County Sheriff's Department had been denied. The ACLU said that this network adds 3 million scans *each week* to a database shared with dozens of other agencies that now includes details from more than *455 million encounters*.

Since about 7 in 10 law enforcement agencies now use LPRs to some degree (and that number is growing all the time), privacy advocates are fighting more aggressively for public access to LPR files. The battle lines are clear: On one hand, the civil libertarians fear government overreach and invasions of privacy. On the other hand, law enforcement officials repeatedly deny misuse of their systems and argue that tracking and storing the data is essential in the fight against crime and terrorism. As an example, scanned vehicle information was essential in tracking down the Boston Marathon bombers, leading to the death of one and the capture of the other.

Maryland in the Vanguard

Sixty-four law enforcement agencies in Maryland use LPR systems. The data collected by these agencies is networked to the Maryland Coordination and Analysis Center ("MCAC"), where it is retained on a central server for one year. Created in the wake of 9/11, MCAC was Maryland's response to the call by the U.S. Attorney General that the U.S. Attorney's Office in every State create an Anti-Terrorism Advisory Council ("ATAC"). The Maryland ATAC formed one of the first Fusion Centers in the United States to combine information sharing and analysis. That center became MCAC. Today, the MCAC coordinates the efforts of federal, state and local agencies to gather, analyze, and share intelligence information with law enforcement, public health, and emergency responder personnel. Until this year, however, the operation of local LPR systems has not been regulated by State law. That changed on May 2, 2014, when Governor O'Malley signed Senate Bill 699 into law. This law, which goes into effect on October 1, 2014, specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and use of "captured plate data." MCAC, in cooperation with the Maryland Chiefs of Police Association and the Maryland Sheriffs Association, must develop a model audit policy for access to and use of LPR data by October 1, 2015.

The procedures to be adopted under the law must include: (1) an identification of MCAC or law enforcement agency personnel who are authorized to query captured plate data gathered by an LPR

system; (2) an audit process to ensure that information obtained through the use of an LPR system is used only for legitimate law enforcement purposes including audits of requests made by individual law enforcement agencies or an individual law enforcement officer; and (3) procedures and safeguards to ensure that MCAC staff with access to the LPR database are adequately screened and trained.

As to the law enforcement agencies themselves, they may not use captured plate data unless the agency has a "legitimate law enforcement purpose," which is defined as the investigation, detection or analysis of a crime or a violation of the Maryland vehicle laws or the operation of terrorist or missing or endangered person searches or alerts. An employee of a law enforcement agency who violates the law's provisions is subject to maximum penalties of imprisonment for one year and/or a fine of $10,000.

And, critically, the new law specifically precludes information gathered by automatic license plate readers systems from disclosure under the Maryland Public Information Act.

In sum, Maryland has enacted a law that in many ways achieves a middle ground that balances privacy interests with law enforcement's interest in license plate reader technology and data. Many states have taken other approaches, including censorship, arbitrary retention policies or an outright ban on LPRs.

What We Must Do Now and in the Future

That LPR technology is a tremendous aid in law enforcement and prevention of terrorism cannot rationally be disputed. Arguments to the contrary simply ignore the benefits of the technology. Rather, it is the protection and use of the scanned information that is at the forefront of the battles ongoing and to come. In fact, as to the DPPR and Maryland's new License Plate Readers and Captured Plate Data law, proper access controls and security of the data are paramount.

As to the DPPA:

Make sure the law's essentials are included in your police/law enforcement agency's manual of rules and regulations. The essentials include what the statute allows, and, just as importantly, what it prohibits. Police access to, and use of, DMV data must be for a legitimate law enforcement purpose. Departmental policies must establish that violation of the DPPA by police officers is a violation of federal law and will expose the officer to administrative review and potential discipline. Officers should receive in-service training based upon the *Rasmusson* case so that they understand that they may be exposed to civil liability for unauthorized "snooping" in DMV records. Periodic training on the ethical use of computers and databases is also necessary.

Finally, if you are incorporating DMV information into traffic tickets/citations, including parking tickets, be prepared to offer concrete reasons why such information is necessary for inclusion in the ticket or citation. The *Senne* case discussed above offers the best discussion of this issue. Also, in Maryland, § 26-201 of the Transportation Article of the Annotated Code of Maryland (2012 Repl. Vol.), must be reviewed. This law requires a traffic citation to contain (in addition to the violation or violations charged, and whether the offense is a payable or must appear violation), the name and address of the person, the number of the person's license to drive (if applicable), and the State registration number of the vehicle (if applicable). However, if a parking ticket is issued for a violation of a local parking ordinance only, *the content requirements of § 26-201 do not apply*.

As to License Plate Reader Networks:

With our new law, Maryland local governments and police agencies are at the forefront of the issues and concerns raised in this publication. They must not delay in addressing them. If not dealt with proactively now, they will be forced to do so later by judicial intervention and decree. If your police agency is using LPRs to any degree (even one), the department must adhere to Maryland's new law that goes into effect on October 1, 2014. Policies and procedures must establish that data acquired through LPRs can only be accessed for legitimate law enforcement purposes. Further, proper auditing controls must be established so that the agency can report annually on their usage of data acquired through LPRs to ensure proper management and oversight of their systems.

You do not need to work in a vacuum. **Attached is a Model Audit Policy for Access to and Use of Automatic License Plate Reader Data (Attachment A).** This model was developed in conjunction with Maryland's new law and should be utilized by every agency using LPR technology.

SOURCES:

Tami Abdollah and Elliot Spagat, *License Plate Scanner Networks Capture Movements*, www.kirtotv.com, http://bigstory.ap.org/article/895e748e8e1449fb810c63e133fc5441/privacy-groups-take-2nd-hit-license-plate-data, September 22, 2014.

Anne Rasmusson, Ex-Cop, Wins $1 Million Lawsuit After Colleagues Database to Look at Her Photo ID, www.HuffingtonPost.com, http://www.huffingtonpost.com/2012/11/07/anne-marie-rasmusson-cop-lawsuit_n_2088239.html?utm_hp_ref=email_share, November 7, 2012.

Thomas Bullock, *Driver's License Snooping*, Virginia Municipal League Insurance Programs, Law Enforcement Matters, Quarterly Newsletter: Fall 2013.

Maggie Clark, *License Plate Readers Spark Privacy, Public Safety Debate*, U.S.A. Today, http://archive.app.com/print/usatodayarticle/3650273, November 20, 2013.

Shawn Musgrave, *Boston Police Halt License Scanning Program*, The Boston Globe, http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-licence-plate-readers-amid-privacy-concerns/B2hy9UIzC7 KzebnGyQ0JNM/story.html? comments=all&sort =HIGHEST_RATING, December 14, 2013.

Ellen Nakashima and Josh Hicks, *Homeland Security is Seeking a National License Plate Tracking System*, Washington Post, http://www.washingtonpost.com/world/national-security/homeland-security-is-seeking-a-national-license-plate-tracking-system/2014/02/18/56474ae8-9816-11e3-9616-d367fa6ea99b_story.html, February 18, 2014.

Opinion/Editorial: Secrecy in License Plate Scans Ripe for Abuse, www.DailyProgress.com, http://www.dailyprogress.com/news/local/opinion-editorial-secrecy-in-license-plate-scans-ripe-for-abuse/article_ace968d8-4255-11e4-ac8b-0017a43b2370.html, September 22, 2014

Dennis Robaugh, *Police Records No Longer Open in Many Communities*, www.Patch.com, http://patch.com/wisconsin/greenfield/police-records-no-longer-open-in-many-communities_d319eda7#.VCl1lFfgXCc, May 7, 2013 (original), October 15, 2013 (updated).

Senate Bill 699, Maryland General Assembly, (2014), http://mgaleg.maryland.gov/2014RS/bills/sb/sb0699t.pdf

Brian Shockley, *Maryland Protects Privacy with License Plate Reader (LPR) Legislation*, www.VigilantSolutions.com, http://vigilantsolutions.com/legislation/maryland-protects-privacy-with-license-plate-reader-lpr-legislation, May 2, 2014.

Neal Ungerleider, *Cisco Gains Traction in the Connected Road Race*, www.FastCompany.com, http://www.fastcompany.com/3026690/internet-of-things/cisco-gains-traction-in-the-connected-road-race, February 20, 2014.

Attachment A

MODEL AUDIT POLICY FOR ACCESS TO AND USE OF AUTOMATIC LICENSE PLATE READER DATA

Introduction

Automatic License Plate Recognition (ALPR) systems, also known as License Plate Reader (LPR) systems, provide automated detection and image capture of license plate information. The LPR system consists of high-speed cameras, mounted either at a fixed location or on a mobile patrol vehicle, and a computer to convert data from electronic images of vehicle license plates into an electronically readable format, which then compares the information against specified databases of license plates. If there is a match is detected, an audible sound occurs and a visual alarm shows the license plate image with the linked information. The system attaches camera identification, date, time, and location information, to include GPS coordinates to the digital image. The image is then maintained electronically in a central location.

The Maryland Coordination and Analysis Center (MCAC) operate a central server to upload and store, read and alarm LPR data from law enforcement agencies across the state of Maryland.

In 2014 Maryland Legislators replaced language in Maryland Annotated Code, Sections 3-509 and 4-326 to address authorized uses of Automatic License Plate Readers and captured plate data. As a result, Maryland law enforcement agencies and the MCAC must implement certain procedures and regulations. This law goes into effect October 1, 2014.

According to Maryland Annotated Code, Section 4-326 the Maryland Coordination and Analysis Center (MCAC) with the cooperation with the Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriff's Association (MSA) have developed this audit policy for access to and use of automatic license plate reader data.

The audit procedures in this policy have been developed to assess the performance of agencies responsible for the operation of LPR systems within their jurisdiction. To assess agency performance, auditors will review policy and procedures regarding the proper use of LPR technology/systems.

Reporting requirements and audit results are due to the State Judicial Proceeding Committee, the House Judiciary Committee, and the Legislative Policy Committee, based on data from the previous year on or before March 1 of each year beginning in 2016.

Purpose

The purpose of this policy is to establish the *[name of agency]* with audit guidelines for assessment of access to and use of Automatic License Plate Reader data.

Policy

This policy applies to all personnel assigned to the *[name of agency].*

Responsibilities

The *[Head of agency]* has overall responsibility for implementation of procedures as it relates to access to and use of Automatic License Plate Reader systems and data. This includes ensuring appropriate personnel are screened and trained in the use of LPR systems.

The *[Head of agency]* will have overall responsibility for LPR data collected or storage by their agency.

The *[Head of agency]* will designate an *[LPR Program Manager/Coordinator]* for the day to day operations of the LPR Program.

The *[Head of agency]* will implement audit procedures to include appointment of auditor and identification of certifying official.

The *[Head of agency]* will have responsibility for submission of audit results to certifying official and will have responsibility to present results of certified audit to appropriate legislative entities.

The [LPR Program Manager/Coordinator] will oversee daily operations of *[name of agency]* LPR Program. The *[LPR Program Manager/Coordinator]* will ensure records relating to access to and use of information within an LPR database are available for audit.

An Auditor(s) will have responsibility for implementing audit procedures, conducting reviews of appropriate documents and records, interviewing appropriate personnel, and reporting results of audit to [Head of agency].

The Certifying official is responsible for validating results of audit. This includes ensuring audit procedures are followed, appropriate reviews were conducted, and audit documents conform with generally accepted audit practices. The Certifying official shall not be associated with the operation of the LPR Program; this official should not be assigned to [name of agency].

Authorized LPR database users are responsible for full cooperation with auditors.

General Procedures

Access to data captured, stored, generated, or otherwise produced by LPR technology shall incorporate safeguards that provide system security and ensure only authorized users are accessing the data for legitimate law enforcement purposes. Each agency must adopt an audit process to ensure that only authorized users are accessing and sharing captured plate data for legitimate law enforcement purposes.

Agencies shall ensure that an audit trail is maintained with respect to compliance to all laws and regulations. Such audit trail shall include an electronic or written record to be maintained as verification that captured plate data is being accessed and used for legitimate law enforcement purposes. These records will be made available to auditors upon request for purposes of conducting inspections and to evaluate compliance with policy, procedures and law. The records to be maintained for the audit are:

- Which personnel in the MCAC or a Law Enforcement Agency are authorized to query captured plate data gathered by an Automatic License Plate Reader system (Maintain record of users who have the "right to know" and the "need to know").
- Procedures and safeguards to ensure that agencies with access to the Automatic License Plate Reader Database are adequately screened and trained (Maintain records of all training curricula for relevancy and proficiency affirmation)
- Individual requests made by any Law Enforcement Officer or Agency for historical data collected by an LPR system or stored in an LPR database operated by the MCAC or any Law Enforcement Agency.

An example of recommended language for use in LPR Policy development addressing the training and audit trail requirements for use in auditing may be found in Appendix B.

Compliance Auditing

Each agency shall submit to an annual audit and shall include the elements of compliance. The audit will provide the following basic objectives:

- Reasonable assurance appropriate control systems have been established by the agency administrator to ensure compliance with laws and rules.
- Reasonable assurance that those with access to and use of LPR data have been properly screened and trained.
- Reasonable assurance the agency has instituted sufficient controls to guarantee queries are for legitimate law enforcement purposes.

- Reasonable assurance that the MCAC or any law enforcement agency using LPR systems have adopted procedures relating the operation and use of the system.
- Reasonable assurance that requests to query captured plate data, made to the MCAC and each law enforcement agency that maintains an LPR database, were conducted for a legitimate law enforcement purpose.
- Reasonable assurance that the information obtained through the use of an LPR system is shared and/or used for legitimate law enforcement purposes.
- To identify any breaches or unauthorized uses of the LPR database.

Sample audit checklists/worksheets may be found in Appendix C.

Audit Procedure

The *[name of agency]* shall submit to an audit *[quarterly, periodically, or annually]*.

The audit shall consist of a predetermined sample size of all relevant requests of data stored in any LPR database. The sampling shall be a random selection of at least 10 percent of relevant requests from that audit period, but no fewer than 50. In the event the total of requests is less than 50, all requests will be audited.

The following two steps shall be used to assess compliance:

1. Administrative Interview: An interview is conducted with *[identify of staff position]* to review agency procedures relating to the operation and use of LPR systems. To include completion of sample questionnaire in Appendix C.
2. Data Quality Review: In conjunction with the interview, a data quality review is conducted with *[identify of staff position]*. This entails comparison of requests to query the LPR database against agency case files and consultation with agency representatives. The accuracy, completeness, and validity are verified during the data quality review.

Audit results will be captured utilizing various checklists/worksheets. Auditors will compile a report of audit results.

The Auditors report, with appropriate additional documentation (worksheets, etc.), shall be provided to certifying official for validation.

Records containing inaccurate or incomplete data shall be documented by Auditor and provided to *[Head of agency or designee]* for appropriate action.

A record that requires corrective action is categorized as inaccurate, unable to location, or incomplete. Below is a description of each discrepancy:

- *Inaccurate:* Key fields in the LPR query record did not match the report, warrant, investigation or supporting document.
- *Unable to locate:* The report, warrant, investigation and/or supporting documentation that substantiates the LPR query could not be located.
- *Incomplete:* the report, warrant, investigation, or supporting documentation contains additional data that should be included in the LPR request record.

Beginning on or before March 1 of each year [beginning in 2016], the *[name of agency]* shall report to the Senate Judicial Proceeding Committee, the House Judiciary Committee, and the Legislative Policy Committee, and the Legislative Policy Committee, in accordance with 2-1246 of the State Government Article, on the lists of audits that were completed.

Appendix A

Definitions

Captured Plate Data: The dates, times, and characters appearing on a license plate, photographs, global positioning system coordinates, and any other data collected by or derived from an Automatic License Plate Recognition System. Captured plate data includes both active and historical data.

Historical Data: Any data collected by an LPR system and stored for future investigative or analytical use. The database which houses historical data may contain, but is not limited to dates, times, and characters appearing on a license plate, location of the read and an image of the individual motor vehicle license plate. Any data collected by an LPR system in accordance with this policy shall be considered collected for a legitimate law enforcement purpose.

Law enforcement Agency: A governmental police force, sheriff's office, security force or law enforcement organization in the State, a county, or a municipal corporation that by statute, ordinance, or common law is authorized to enforce the general criminal and traffic laws of the State.

Legitimate Law Enforcement Purpose: Applies to the access of Active or Historical Data and means the investigation, detection, analysis or enforcement of a crime, violations of the Maryland Motor Vehicle Administration (MVA) laws, for the operation of AMBER, SILVER or BLUE alerts for missing, endangered, or wanted person searches, terrorist watch list alerts, and for public safety. NOTE: "Legitimate law enforcement purpose" does not include video tolling, a technique using video or still images of a vehicle's license plate to identify the vehicle for payment.

Maryland Coordination and Analysis Center (MCAC): Is Maryland's Fusion Center which coordinates the efforts of federal, state, and local agencies to gather, analyze, and share information with law enforcement, public health, and emergency management personnel.

Appendix B

Sample Language for Establishing Training requirements and an Audit Trail within agency LPR Policy

The *[name of agency]* uses and has access to data captured, stored, generated, or otherwise produced by LPR technology. Safeguards are in place to provide system security and ensure only authorized users are able to access the data for legitimate law enforcement purposes.

It is the responsibility of *[identify a staff position(s)]* to ensure only appropriate staff have access to necessary systems and portals for LPR systems and captured plate data.

The *[name of agency]* will ensure that *[identify of position/unit]* is properly trained on the use of LPR systems and captured plate data. Staff is required to complete the following training prior to accessing any LPR systems: *[List all training requirements]*

Training #1: Proper use of Car System

Training #2: Proper use of Operations Center

The only authorized users are *[identify the position/unit]*

An audit trail shall be kept for all Individual requests for historical data stored in an LPR database operated by *[name of agency]*. The following information shall be maintained.

1. Date and time of the request; and
2. Purpose of the request; and
3. Incident or report number (physical record number) related to the query; and
4. The identity of the agency requesting the query (including if the requester is from a local, state, federal or out-of-state agency); and
5. The requester's name and contact information; and
6. The license plate number or other data elements used to query the LPR system.

The audit trail of requests shall by maintain for *[period of time]*.

Appendix C

SAMPLE AUDIT QUESTIONS (Step 1)

Goal	Question	Answer	Comments
1	Have procedures been adopted relating to the operation and use of the LPR system? [Cite policy number]	YES NO	
2	Are staff with access to the Automatic License Plate Reader database adequately screened and trained?	YES NO	
3	Does the agency maintain training records for each user?	YES NO	
4	Is the training curricula maintained?	YES NO	
5	Are training records annually reviewed for relevancy and effectiveness?	YES NO	
6	Does the agency accept law enforcement requests for historical plate data, collected by an LPR system?	YES NO	
7	If historical data is accessed, does the agency have an audit trail?	YES NO	
8	Is the audit trail maintained for 2 years?	YES NO	
9	Have audit procedures been adopted to ensure that information obtain through the use of an LPR system is used for legitimate law enforcement purposes?	YES NO	
AGENCY:		SCOPE OF AUDIT:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	

SAMPLE AUDIT QUESTIONS (Step 2)

	Question # 1	Question #2	Question # 3	Question # 4	Question #5	Results
Record #	Report/Incident Number	Is the date and time of request documented?	Is the purpose of the request documented?	Does the request include the identity of the agency requesting the query?	Has the request been validated through the requesters agency?	Findings shall be listed as: Accurate, Inaccurate, Unable to locate or Incompletd
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35