

SYRACUSE SCIENCE AND TECHNOLOGY LAW REPORTER

Automatic License Plate Recognition: An Exciting New Law Enforcement Tool with Potentially Scary Consequences

Tyson E. Hubbard¹

INTRODUCTION

How would you feel if your daily travels were tracked and stored in a large computer database? Presumably someone going over the raw data could figure out where you worked, where your kids went to school, where your family lived and at what stores you liked to shop. In the wrong hands, the potential abuses of that sort of information are very scary. What many people do not realize is that it is exactly this type of information that is being collected every day by police officers across the country. New technology which is being heavily marketed to police departments allows a camera mounted on top of a police cruiser to take a picture of your license plate and store that information, complete with time, date and exact latitude and longitude coordinates for your vehicle. This sort of information is gathered anytime your car happens to travel past a police car, or more accurately anytime a police car travels past your car. Think about how many times you pass a police car on the average day: maybe it is on the freeway, or you see a police officer doing speed checks, or you are even going the other direction on the freeway and there is an officer across the median. Maybe as you run your daily errands there is police car that has someone pulled over on the side of the road, or even a cruiser parked at the

¹ J.D. Candidate, Syracuse University College of Law, 2008; Executive Editor, *Syracuse Science and Technology Reporter*. He would like to thank his parents, Clifton and Jacqueline Mills and Larry Waterman, as well as Jessica Stannard-Friel, for their tremendous support.

local donut shop. Then there are the times a police officer drives by your car and you are not even aware. You might be in the parking lot at work or home with the garage door open. Every time a transaction like this occurs, when your car and a police car are in the same location and the officer's camera is operational, the information is collected. With the vast amount of information being collected and stored on every driver, police departments across the country have essentially placed tracking devices onto everyone's vehicles.

The technology is called Automatic License Plate Recognition (ALPR), and it was first developed in Britain in an attempt to slow the operations of the Irish Republican Army which, at the time, had used car bombs in terrorist attacks.² ALPR is comprised of cameras on top of a police cruiser.³ As the car drives along the road, the cameras take infrared pictures of the license plates on cars traveling ahead of and behind the police car.⁴ Additionally, side cameras are able to take pictures of cars parked on either side of the road or cars being passed on the freeway.⁵ The camera images are then sent to a computer which converts the pictures into text and cross-references against a list of stolen cars, known criminals, arrest warrants, and those who have outstanding parking fines.⁶ If there is a hit, then an audible alarm in the cruiser signals the police officer.⁷ The system is so advanced that an alarm also goes off in the police station and

² Kevin Gordon, *Automatic License Plate Recognition*, 54 LAW & ORDER 5, May 2006, available at 2006 WLNR 10638833.

³ William Murphy, *View From the Top: Cops can easily read ID license plates of cars involved in crime with new roof-mounted scanning system*, NEWSDAY, Apr. 6, 2006, at A3.

⁴ *Id.*

⁵ *Id.*

⁶ Gordon, *supra* note 2.

⁷ Murphy, *supra* note 3.

dispatchers can determine whether or not back-up might be needed.⁸ The cameras can process thousands of license plates per 8-hour shift.⁹ In addition to an alarm in the cruiser, the system records the time, date and coordinates of where the plate was scanned.¹⁰ The system allows the police to check and see if “a vehicle was at a certain place at a certain time.”¹¹ While the system is designed to catch criminals who have already committed devious acts, the recording feature stores information about non-criminals. The collection of this information is justified on the basis that it can be used to establish patterns of movements for a criminal or even to locate potential witnesses in the vicinity of a crime.¹² After a crime is committed and a suspect is identified, it is much easier to locate that criminal if the police can tap into their databases and discover where the suspect resides and the locations the suspect has previously visited. At the very least, such geographic information helps to develop a pattern for a jumping-off point for an investigation. Of course, with the quantity of information collected, and the availability of data points on all cars, and thus all drivers, it is easy to see how the system can be abused.

This note will first look at the technology and show why police departments around the country are so excited about the ability of this equipment. Next, the note examines the constitutional issues involved with using this sort of license plate reading technology and a few legal issues which the software may need to overcome in order to be accepted by the general public. Finally, the note argues that even if the technology is entirely legal and constitutional,

⁸ *Id.*

⁹ *Id.*

¹⁰ Carol Robinson, *Deputies to deploy plate ID system: System compares car tags, databases to expose criminals*, BIRMINGHAM NEWS, Mar. 24, 2006, at 1C.

¹¹ *Id.*

¹² Tim McFadden, *Automatic License Plate Recognition System Emerge as a Law Enforcement Tool*, OFFICE OF LAW ENFORCEMENT TECHNOLOGY COMMERCIALIZATION, Apr. 2005, available at http://www.oletc.org/oletctoday/0415_licplate.pdf#search=%22%22automatic%20license%20plate%20recognition%22%22.

there is a need for safeguards to be put in place to protect the public from abuse of the system by third-parties or inappropriate police abuses.

REVOLUTIONARY POLICE TECHNOLOGY: JUST WHAT IS SO GREAT ABOUT AUTOMATIC LICENSE PLATE RECOGNITION?

Police have been running license plates practically since they were implemented. License plates have been required in New York State since at least 1904.¹³ In New Jersey, and no doubt many other states, license plate numbers were originally issued to automobile owners, and then it was the owner's responsibility to hire a craftsman to construct the plate.¹⁴ One obvious reason that license plates exist is to provide some clue as to the identity of the driver. Not only can a driver's identity be ascertained by the public at the scene of an accident, but with the advent of radio communications, license plates allowed the police to "check up" on a driver through their license plate. Before computers, police could "call" a plate number in on their radio and check the status of any licensed vehicle to see if it was stolen or if the registered owner had any outstanding warrants. But as technology advances all around us, so it also advances for law enforcement professionals.

This new Automatic License Plate Recognition technology allows the police to collect and process license plates in a scope never before imagined. In British Columbia, the Integrated Municipal Provincial Auto Crime Team has just started to use ALPR.¹⁵ They have equipped six cars, five unmarked, that each will be able to scan 600 license plates an hour.¹⁶ In Nassau

¹³ License Plates of the World, http://www.worldlicenceplates.com/jpglps/USA_NY_GI1_1900's-10's.jpg (last visited Mar. 25, 2007).

¹⁴ State of New Jersey – Motor Vehicle Commission – Vehicles, <http://www.state.nj.us/mvc/Vehicle/Plates.htm> (last visited Mar. 25, 2007).

¹⁵ Matt Kieltyka, *Bait-car program to grow*, 24 HOURS, Vancouver Edition, Nov. 16, 2006, at 5.

¹⁶ Matt Kieltyka, *High-tech police work: LICENSE PLATE RECOGNITION*, 24 HOURS, Vancouver Edition, Nov. 14, 2006, at 5.

County, New York, the system is able to scan 8,000-10,000 license plates during an officer's eight-hour shift.¹⁷ Police Chief James Russo said, "[i]t's like having 10 cops out there looking for stolen cars."¹⁸ Motorola, which makes one of the systems, says that it has at least two dozen police department using its system in fifteen different states, including the Yonkers and Chicago Police Departments.¹⁹ It is clear that the use of ALPR is growing across North America.

The system is not easily deterred from getting license plate numbers. In a press release, Extreme CCTV Int'l Inc. boasts that its product can scan license plates "under any lighting condition, from total darkness to direct glare from high-beam headlights, capturing plates from vehicles moving at up to 120 kph (75 mph)."²⁰ A new system to be put in place in Winnipeg can scan 200 plates in a single minute.²¹ That system compares to one plate per two minutes the "old-fashioned" way.²² Additionally, the Winnipeg system can recognize the indentations of the numbers to enable the computer to read plates covered in mud or plates that have been painted over.²³ In Jefferson County, Alabama, the equipment costs approximately \$20,000 per unit, but can scan "thousands of license plates an hour."²⁴ In Alabama, the system links to a database of

¹⁷ Murphy, *supra* note 3.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Camera provides license plate capture up to 120 ft. (Extreme's REG-ZI Achieves Effective License Plate Capture Up To 120ft)*, PRODUCT NEWS NETWORK, Oct. 23, 2006, available at <http://news.thomasnet.com/fullstory/496753..>

²¹ Bruce Owen, *Car thieves have new enemy: Police camera scans 200 plates per minutes*, WINNIPEG FREE PRESS, Mar. 23, 2007, at B1.

²² *Id.*

²³ *Id.*

²⁴ Robinson, *supra* note 10.

stolen cars, drug dealers, wanted felons and convicted pedophiles from the states of Alabama, Tennessee and Georgia.²⁵

In addition to cruiser mounted models, the Arcadia (California) Police Department has purchased stationary license plate scanners.²⁶ The stationary cameras were to be mounted at the entrance to the Santa Anita Racetrack as well as the local mall, and will scan every car that enters or exits those venues.²⁷ The Regional Manager of the company which makes the system said that the camera has the ability to scan 1,500 plates per hour, while “a diligent police officer might run 60 to 80 plates per hour.”²⁸ Those numbers indicate that a single license plate recognition computer system is doing the work of 20 to 25 “diligent” police officers every hour! In a test run of the system by the California Highway Patrol the officers recovered 26 stolen vehicles and arrested seven people in twenty days.²⁹ Without the equipment over a similar time period, the California Highway Patrol averages 2.3 cars recovered and may not have made a single arrest.³⁰ As Arcadia Police Chief Bob Sanderson pointed out, the license plate scanners greatly increase the reach of law enforcement.³¹ Similarly, positive results were seen during a test run in Maryland. There, the Maryland State Police “recovered 8 cars, found 12 stolen plates, and made 3 arrests in just one shift while field-testing the equipment.”³² It is clear that these

²⁵ *Id.*

²⁶ Marshall Allen, *Plate scanner to aid Arcadia police*, PASADENA STAR-NEWS, Sept. 5, 2005, at A-1.

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ Allen, *supra* note 26.

³² McFadden, *supra* note 12.

systems were highly effective in their test runs at out-performing traditional police work and in a more cost-effective fashion.

The technology can easily detect more than just stolen vehicles and criminals. In Philadelphia, the police are using the system for more than hardened criminals and stolen cars. There, they have equipped a Chevy Venture van with the license plate scanning equipment in an attempt to find those who owe old parking tickets.³³ The van “creeps” through the City streets and will *only* scan around 3600 plates per day.³⁴ In Houston, which uses the same system, the van is able to find around a dozen parking violators per week and boot the cars.³⁵ “Old fashioned” parking enforcement would require 20 officers to find that many violators in a single week.³⁶ Again, the system pays off as a way to cheaply replace expensive human labor while at the same time increasing the number of tickets that are written and fines that are assessed.

The system’s scanning technology can be used in a number of ways to benefit police departments nationwide. In an environment of budget cuts, the ability to replace a substantial amount of manpower with relatively cheap computer systems must be appealing to many police chiefs. They can catch more criminals with less overhead costs. When the substantial size of a human police force, which requires salary, healthcare costs, and pensions, can be replaced by a one-time purchase of relatively inexpensive technology, then costs go down. Using this system effectively not only reduces costs but, given its efficiency at finding parking offenders and other criminals, the system should lead to an increase in revenue as more traffic ticket fines are paid and those parking violations which have already been assessed are collected.

³³ Mitch Lipka, *Traffic Scofflaws, Watch Out*, PHILA. INQ., Sept. 22, 2006, at B-01.

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

But like everything, for every action, there will be a separate but equal reaction. With the numerous benefits of the program come some clear and potentially scary drawbacks. While it is easy to see that there are great benefits to finding stolen cars and forcing those people who ignore their parking tickets to pay up, there exist scary consequences for the majority of us who proceed through our daily lives without breaking any laws. Why are the police keeping track of our everyday movements? The general public, the vast majority of us, have committed no crimes and have done nothing wrong. Why are the police allowed to track the movements of entirely innocent people and store personal information like the exact time, date and location of your vehicle at any given moment?

Unfortunately, there is the opportunity for abuse. Imagine the plight of the police chief's teenage son. He had better really go to the library when he tells his dad that's where he's headed. The officer would hypothetically be able to check the computer system and see exactly what locations his son's car was spotted at and at exactly what time. This relatively light hypothetical provides for a largely harmless abuse; however, the potential for more serious abuses by the police are plenty. Worse than any law enforcement overstep, imagine if the information fell into the wrong hands. What if a devious police officer wanted revenge on an enemy, or someone at the station gained access to the information for their own nefarious means? This information is no doubt stored in an electronic database and consequently could be subject to hacking by any number of criminals for any number of reasons. A stalker would be allowed a unique glimpse into the precise movements of his victim. Even a major corporation might like access to the information to determine what types of drivers are in what sorts of locations at what times. While clearly there are benefits to using these automatic license plate readers, it is important to weigh both sides of the issue and consider the drawbacks to this system

before jumping headlong into a widespread purchasing plan and implementing this technology in police departments across the nation. In addition to these policy reasons, which may indicate hesitancy in supporting this technology, it is also important to consider many constitutional issues at play.

CAN THE POLICE CONSTITUTIONALLY COLLECT AND KEEP THIS INFORMATION?

It is worth exploring the constitutional issues prevalent with this technology to decide if the use of these systems is even legal before considering whether the use of the systems is appropriate. Two constitutional issues to examine include the effect of this technology on the right to travel, implicating the Privileges and Immunities Clause of Article Four, and the right to remain free from unreasonable searches and seizures under the Fourth Amendment.

A. A System Of Aggressive Enforcement Through Automatic License Plate Recognition Burdens Travel, But Does Not Discriminate Against A State's Non-Residents And Therefore Is Not In Violation Of The Privileges And Immunities Clause

In 1999, the Supreme Court reaffirmed that a right to travel exists within the Constitution.³⁷ It was a conclusion that the Court had reached in prior rulings, including *United States v. Guest*, where the Court held, “[t]he constitutional right to travel from one State to another, and necessarily to use the highways and other instrumentalities of interstate commerce in doing so, occupies a position fundamental to the concept of our Federal Union.”³⁸ The Privileges and Immunities Clause of Article Four of the Constitution is often invoked when dealing with the right to travel. The clause reads, “[t]he Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States.”³⁹ In *Saenz*, the Court ruled

³⁷ See *Saenz v. Roe*, 526 U.S. 489 (1999).

³⁸ 383 U.S. 745, 757 (1966).

³⁹ U.S. CONST. art. IV.

against a residency requirement for welfare benefits finding a “right of the newly arrived citizen to the same privileges and immunities enjoyed by other citizens of the same State.”⁴⁰ In *Guest*, the Supreme Court concluded that “[t]he right to travel...has been firmly established and repeatedly recognized.”⁴¹ If intrusive license plate scanners overzealously burden the ability of free movement between the states then that technology may be found to interfere with the right to travel.

While no cases have specifically looked at the issue of mass automatic scanning of license plates, one leading case on the subject of manually inputting license plates held that license plate checks do not interfere with interstate travel. In a case from the Tenth Circuit, a law enforcement officer performed a random license plate check on an out-of-state 1983 Cadillac.⁴² When the license plate came back belonging to a 1988 Toyota, the officer activated his lights and stopped the car.⁴³ As it turned out the radio dispatcher had transposed the numbers in the license plate given to him by the officer and in fact there were no problems with the properly plated Cadillac when the dispatcher ran the correct plate number.⁴⁴ However, the officer remained suspicious of the two passengers of the vehicle and performed a search in which the officer found two kilograms of cocaine.⁴⁵ On appeal, the defendants claimed that the officer’s license plate check of their vehicle violated the Privileges and Immunities Clause because it burdened

⁴⁰ 526 U.S. at 502.

⁴¹ 383 U.S. at 757.

⁴² *United States v. Walraven*, 892 F.2d 972, 973 (10th Cir. 1989).

⁴³ *Id.*

⁴⁴ *Id.* at 974.

⁴⁵ *Id.*

their right to interstate travel.⁴⁶ The District Court of Wyoming found no violation, and the Tenth Circuit agreed, holding, “[the officer’s] registration check on [the driver’s] Cadillac neither unreasonably burdened nor restricted [the driver’s] travel. Unless a registration check reveals information which raises a reasonable suspicion of criminal activity, the subject remains unaware of the check and unencumbered.”⁴⁷ The Circuit expressly agreed with the District Court’s holding, quoting that decision: “[i]n view of the manner in which the license checks are conducted, the extent of any intrusion upon the traveling public . . . hardly rises to an impermissible interference with the fundamental right to travel from state to state.”⁴⁸ According to the court, since the police officer’s act of reading a license plate off of a vehicle traveling in front of him and checking the validity of the plate with a dispatcher goes unnoticed by driver as long as there are no problems, then the driver’s right to travel has not been burdened.⁴⁹ Essentially, what the driver doesn’t know can’t hurt him.

The court in *Walraven* reached the conclusion that the mere act of checking a license plate was not so much of a burden as to constitute a violation of the fundamental right to travel.⁵⁰ This process would work in the exact same way whether the officer was manually typing the license plate number into his computer or if he allowed a camera on his roof to take a picture and convert the picture to text. Further, once the officer has a hit on a suspicious vehicle and decides to pull the car over, if this action unnecessarily burdened the fundamental right to travel, it is likely that the government would have a compelling reason for infringing on that right. If

⁴⁶ *Id.*

⁴⁷ *Walraven*, 892 F.2d at 974.

⁴⁸ *Id.* (citing *United States v. Pitchford*, 699 F. Supp. 260, 264 (D. Wyo. 1988)).

⁴⁹ *Walraven*, 892 F.2d at 974.

⁵⁰ *Id.*

someone's travel was actually delayed or burdened, it would only be because they were pulled over on account of some red flag in the computer system. If the car was stolen or there was a warrant for the driver's arrest, then burdening these people would be permissible because there would be compelling governmental interest in the action. If instead the system notified the officer every time he passed an out-of-state driver, whether or not there were any violations attached to the driver, then the likelihood of finding the technology unconstitutional would definitely be increased.

Finally, it is unlikely that the Privileges and Immunities Clause would hamper the operations of Automatic License Plate Recognition technology because there is no distinction drawn between in-state and out-of-state residents. If anything, out-of-state residents are afforded more protection because it is likely that police cruiser computer systems are not linked into databases from other states. An out-of-state resident with a scattered driving history might be more likely to avoid detection while operating in another state because the ALPR system might not include his home state's violations.

Because the process of checking a license plate does not burden an innocent driver, the Automatic License Plate Recognition technology only notifies the officer when the government would have a compelling reason to burden travel. Further, the system treats out-of-state drivers no worse than in-state resident drivers. Because of these reasons, it is unlikely that checking license plates, either manually or with an ALPR system, would constitute a violation of the privileges and immunities clause.

B. The Supreme Court's *Katz* Test Requires Both An Objective And Subjective Expectation Of Privacy Before A Search Is Unconstitutional Under The Fourth Amendment

Given the long history of the nation, it is somewhat surprising that the Supreme Court has only recently begun to develop clear rules concerning an individual's right to privacy. There is

no right to privacy expressly outlined in the Constitution. However, the Fourth Amendment provides, “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...”⁵¹ Much of the law concerning an individual’s right to privacy and its relation to constitutional searches under the Fourth Amendment stems from *Katz v. United States* in which the Supreme Court articulated a two-part, objective and subjective, test for the right to privacy.⁵²

In *Katz*, a Los Angeles man was arrested and charged with transmitting wagering information after the FBI bugged the public telephone that he often used to place these calls.⁵³ The oft-quoted “Katz Rule” emerged from the concurrence written by Justice Harlan stating that the Fourth Amendment offers protections of privacy where “a person [has] exhibited an actual (subjective) expectation of privacy and... the expectation [is] one that society is prepared to recognize as ‘reasonable.’”⁵⁴ The test requires both an objective and subjective expectation of privacy. Applying his newly stated rule to the *Katz* case, Justice Harlan found that a person who enters a telephone booth and shuts the door behind him has an expectation that his conversation is not overheard.⁵⁵ The opposite is true where someone conducts business or commits a crime in an open air free to the view of the public. “As a result, that which is done or said in a space that can be viewed or overheard by a member of the general public is not off limits to law

⁵¹ U.S. CONST. amend. IV.

⁵² See 389 U.S. 347 (1967).

⁵³ *Id.* at 348.

⁵⁴ *Id.* at 361 (Harlan, J., concurring).

⁵⁵ *Id.*

enforcement officials merely because they are an arm of the government.”⁵⁶ When someone does an act in the public’s view, or displays something for the public to see, they should not have a reasonable expectation of privacy. Such an action that takes place in an area open to the public’s eye would fail the objective portion of the *Katz* test, would not be entitled to any privacy protections, and would not constitute an unreasonable search under the Fourth Amendment.

The *Katz* test would need to be applied to license plates in order to determine whether there exists any privacy interest in the information the license plates display which could be violated by the Automatic License Plate Recognition systems. Are there both subjective and objective expectations of privacy in a number stamped in metal and screwed to the outside of your car? Not likely. Established case law dictates that a police officer entering a license plate into a computer is not an illegal search under the Fourth Amendment since license plates displayed in open sight on a car have no expectation of privacy. “To contest the validity of a search, a defendant must demonstrate that he *himself* exhibited an actual subjective expectation of privacy in the area searched, and that this subjective expectation is one that society is willing to accept as reasonable.”⁵⁷ It is hard to imagine how any person would subjectively think that their license plate, exposed for all to see, was deserving of some kind of privacy.

When the objective side of the *Katz* test is considered, the answer is even clearer that there is not a reasonable societal expectation of privacy in license plates. In fact, given the trend toward vanity license plates designed to share a message, it is obvious that license plates are becoming a place for expression and are meant to be noticed. If license plates were truly viewed

⁵⁶ John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 73-74 (2002).

⁵⁷ *United States v. Hill*, 2005 U.S. Dist. LEXIS 31240, at *16 (D. Conn. Nov. 18, 2005), *citing* *United States v. Fields*, 113 F.3d 313, 320 (2d Cir. 1997).

as private, then there would be little point to paying an additional registration fee to have a more noticeable license plate.

C. There is No Reasonable Expectation of Privacy In A Publicly Visible License Plate, Therefore “Running” License Plates Is An Appropriate Search Under The Fourth Amendment

The *Katz* test has been applied to many different factual scenarios, from aerial inspections of marijuana growths⁵⁸ to stolen cars parked in open garages.⁵⁹ The Tenth Circuit has twice articulated that, “[b]ecause they are in plain view, no privacy interest exists in license plates.”⁶⁰ Recently, the Sixth Circuit reached a similar conclusion after applying a *Katz*-like reasonable expectation test to information contained on license plates.⁶¹

In *United States v. Ellison*, a police officer noticed Ellison’s van idling in a “fire lane” next to a shopping center.⁶² The officer decided to observe the van while entering the van’s license plate number into his computer.⁶³ Upon entering the information he learned that the van was registered to Curtis Ellison, an individual with an outstanding felony warrant.⁶⁴ When the van pulled away from the shopping center the officer pursued and eventually pulled the van over.⁶⁵ Ellison was a passenger in the van and the officer notified Ellison that he was being

⁵⁸ See *infra* p. 22-23.

⁵⁹ See *infra* p. 17.

⁶⁰ *Walraven*, 892 F.2d at 974 (citing *United States v. Matthews*, 615 F.2d 1279, 1285 (10th Cir. 1980)).

⁶¹ See *United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006).

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

arrested for an outstanding warrant.⁶⁶ While performing a routine pat down, the officer found two firearms.⁶⁷ Ellison was indicted on a firearms charge but moved for a “motion to suppress under the ‘fruit of the poisonous tree’ doctrine.”⁶⁸ The District Court agreed, finding that the van had not been parked illegally and, therefore, the police officer did not have probable cause to run the van’s license plates through his computer system.⁶⁹ The Circuit Court reversed, finding under the Fourth Amendment that “a motorist has no reasonable expectation of privacy in the information contained on his license plate.”⁷⁰ Referring to the Vehicle Identification Number (VIN), the Supreme Court has held that, “[i]t is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile...The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a ‘search.’”⁷¹ Because license plates are required to be exposed to the public in plain view anyone could read them, including the police.

As both the Sixth and Tenth Circuits have held, license plates are required to be displayed for the purpose of identification by law enforcement, and, therefore, there is no expectation of privacy in the information contained on the plates. Without an expectation of privacy when an officer runs the number through his computer, license plate checks in general are not an unreasonable search under the Fourth Amendment.

⁶⁶ *Ellison*, 462 F.3d at 559.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ *Id.* at 561.

⁷¹ *Ellison*, 462 F.3d at 561.

D. Whenever An Item Is In The Public's View There Can Be No Reasonable Expectation Of Privacy, Even When On Private Property Or In An Open Garage

The holding from *Ellison* may also be true even when a vehicle is on private property. Sometimes there is not an expectation of privacy in a license plate even where a vehicle is off of the street and out of the public's domain; for example, when a car is parked in a garage, but the door is open. The Automatic License Plate Recognition systems have the ability to scan for the plates of cars parked on either side of the road, which could include cars parked in yards, driveways and even inside of garages with the doors open.⁷² Courts are unlikely to make a distinction between a law enforcement officer typing in a license plate read from a car parked in a garage and the ALPR system processing the same information by means of the officer driving by an open garage.

In *People v. Clark*, the Court of Appeals of Michigan held that the scenario described above, where an officer used binoculars to read the license plate of a stolen car in an open garage, was not an unreasonable search.⁷³ "It is firmly established that the law offers no protection to items which a person 'knowingly exposes to the public'."⁷⁴ The Court held that the open garage failed the subjective portion of the *Katz* test as "[the] [d]efendant could not reasonably expect that passers-by would shut their eyes to what was clearly visible from the sidewalk or from across the street."⁷⁵ Whether an officer enhances his vision with binoculars or allows the ALPR system to read the plate for him a court is likely to consider information taken from a car left in open view a reasonable search.

⁷² Murphy, *supra* note 3.

⁷³ *People v. Clark*, 350 N.W. 2d 754, 756-58 (Mich. App. 1984).

⁷⁴ *Id.* at 758.

⁷⁵ *Id.*

Courts are unlikely to make a distinction between an officer processing a plate off of an individual vehicle and the same information being collected from Automatic License Plate Recognition technology. Courts have seemingly taken a hard stance. When an individual vehicle is considered, and that vehicle is in plain sight of any member of the public, then there is no reasonable expectation of privacy and, therefore, checking that vehicle's license plates does not constitute an unreasonable search under the Fourth Amendment.

E. The Use Of Tracking Devices, And Similar Technology, Is Constitutional Where The Same Surveillance Could Have Been Completed With Traditional Police Work

In addition to checking the license plates of vehicles for crimes that have happened in the past or registration to known criminals, the collection and recordation functions related to the Automatic License Plate Recognition systems act to track innocent people in the event that they may commit, or be involved in, a crime in the future. When the computer runs a license plate it enters the exact GPS coordinates, time and date for the license plate. The asserted justification is that if in the future the police are looking for a suspect, or even victim, who owns a specific car, then they could check the database and see where the suspect has been in the last few weeks, or last few moments, to help them begin their search. No case involving the tracking aspects of this software has yet reached a court in this country; however, a few courts have discussed more traditional tracking devices and settled on somewhat surprising conclusions.

In a recent case involving an Upstate New York attorney, a large drug ring and the Hell's Angels Motorcycle Club, the Oneida County Sheriff's Department placed a GPS tracking device on the vehicle belonging to an attorney who was making numerous trips to Arizona to buy methamphetamines.⁷⁶ The GPS device, which was attached without approval or a warrant, tracked the movements of the attorney, Robert Moran, upon his return from one specific trip to

⁷⁶ See U.S. v. Moran, 349 F. Supp. 2d 425 *passim* (N.D.N.Y. 2005).

Arizona.⁷⁷ The court ruled that the police action of attaching a GPS unit to the suspect's car was not an invasion of the suspect's privacy and not an unreasonable search under the Fourth Amendment.⁷⁸ The court determined that driving is by nature a public exercise, and, therefore, a person has no expectation of privacy while they drive their car.⁷⁹ Here, the officers tracked the suspect as he drove over a two-day span.⁸⁰ The court suggests that the technology did not aid the search in any unfair way as "[l]aw enforcement personnel could have conducted a visual surveillance of the vehicle as it traveled on the public highways."⁸¹ As such, the Court found no reasonable expectation of privacy in the whereabouts of the attorney's vehicle and therefore no unreasonable search.

The Court in *Moran* based part of its holding on a 1983 Supreme Court case where a defendant was arrested after the police attached a beeper to a drum of chloroform that he had purchased with the intent to make illegal drugs.⁸² The beeper led the police to the defendant's rural Wisconsin cabin where he was making amphetamines.⁸³ The Supreme Court reasoned that the beeper did not constitute an unreasonable search because "[a] person travelling [*sic*] in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."⁸⁴ The Court also held that this was not an issue of advanced

⁷⁷ *Id.* at 467.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Moran*, 349 F. Supp. 2d at 467.

⁸² *United States v. Knotts*, 460 U.S. 276, 276 (1983).

⁸³ *Id.*

⁸⁴ *Id.* at 281.

technology enabling police to exceed reasonable expectations of privacy because “[a] police car following [the delivery driver] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by [the defendant], with the drum of chloroform still in the car.”⁸⁵ First in *Knotts* and then again in *Moran*, at least two courts have expressly allowed the use of advanced technology to track private citizens without a warrant because of the assertion that traditional police work could have done the job.

Even when technology plays a role, the Court has been hesitant to find an invasion of privacy where traditional police work could still accomplish the same ends.

F. While There May Not Be An Expectation Of Privacy In Any One License Plate, Could The Automatic License Plate Recognition Technology Violate A Right To Privacy That May Exist In A Mass Of License Plates?

Despite numerous courts’ seemingly wholesale disclaimers from finding a privacy right in license plates, or even in daily movements, the case of Automatic License Plate Recognition technology continues to bring up interesting issues, mainly, the comprehensive nature of the searches occurring at any one time. One police officer entering the license plate numbers that he is able to read into a computer is not an intrusive search says the *Ellison* court.⁸⁶ *Knotts* and *Moran* agree that a tracking device is not an unreasonable search where an officer could have followed the suspect just as easily. However, the Sixth Circuit in *Ellison* also referenced a number of decision in which courts questioned the intrusive nature of technology, opening the door for an examination of the possibility of finding an unreasonable search when advanced technology is involved. The cases referred to involve the use of aerial photographs with

⁸⁵ *Id.* at 285.

⁸⁶ *Ellison*, 462 F.3d at 562.

precision aerial mapping cameras⁸⁷ and the use of thermal imaging to see individuals inside of a residence.⁸⁸ The court concluded in dismissing Ellison’s claims that “[t]his is not a case where the police used a technology not available to the public to discover evidence that could not otherwise be obtained without ‘intrusion into a constitutionally-protected area.’”⁸⁹ It seems clear enough that there is not an expectation of privacy in any one given license plate which is exposed to the public for all to see. If there is a police officer parked behind you then he clearly has the ability and opportunity to type your license plate number into his computer and check the status of your vehicle and the registered owner. But, could there be an expectation of privacy in the anonymity provided by driving on crowded freeways? Or parking in a lot where there are so many other cars that it would be virtually impossible for a police officer or even a police department to check all the cars? This new type of technology that allows enforcement on a scale never before imagined destroys any assumptions about the anonymity of driving.

One reason that these systems should be closely monitored is that they greatly increase the scope of police information collecting abilities to a level we have never experienced. Given the vast number of license plates that can be run per shift and the fact that the cameras can catch plates from all angles, is this still a proper use? Isn’t it plausible that the advent of this technology makes the license plate checking process so much more intrusive as to violate a right to privacy?

The use of technology has created new issues related to privacy and reasonable searches. “The Court has consistently ruled that *enhancing* technologies do[es] not constitute [illegal or

⁸⁷ *Id.* (citing *Dow Chemical Co. v. United States*, 476 U.S. 227, 239 (1986)).

⁸⁸ *Id.* (citing *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001)).

⁸⁹ *Id.* at 562.

unreasonable] searches under the Fourth Amendment.”⁹⁰ Examples of enhancing technology include using binoculars to see better and dogs which smell more effectively than humans do. However, the Supreme Court first expressed its nervousness regarding enhancing technologies in *Dow*,⁹¹ when the Environmental Protection Agency (EPA) used airplanes to capture evidence from the skies. As one commenter pointed out in regard to a similar case, “[b]arring an argument that airplanes just expand on our ability to flap our arms, it's hard to see what justifies the intrusion.”⁹² The same could be said of License Plate Recognition. Does the system merely enhance the officer’s ability to see in all directions in complete darkness, read small and distant numbers, correctly in-put a series of digits in seconds, memorize a database of millions of license plates and alert themselves to an offender? It sounds ridiculous, but it is essentially what the ALPR system does for the officer. As a Los Angeles police officer pointed out concerning the technology’s ability to read license plates at 60 mph and at night, “[i]t's physically impossible for an officer to do this kind of work...It's reshaping the way we do policing.”⁹³ If the Supreme Court chooses, as they have in the past, to draw lines between technologies which merely enhance human ability and technologies which are essentially superhuman and not available to the public, then the constitutionality of Automatic License Plate Recognition systems is suddenly in a much more tenuous position.

In 1986, the Supreme Court dealt with two separate cases, both involving over-flights as searches, where the government observed illegal activity in an airplane while flying over a

⁹⁰ Brogan, *supra* note 56 at 77 (emphasis added).

⁹¹ *See Dow*, 476 U.S. 227 (1986).

⁹² Brogan, *supra* note 56 at 77.

⁹³ Jonathon Stroud, *Scanning 'takes the guesswork out of policing'*, DAILY BREEZE (Torrence, Calif.), May 7, 2006, at A1.

suspect's property. First, in *California v. Ciraolo*, the Court held that a high fence around a crop of marijuana did not clearly meet the *Katz* subjective expectation of privacy test where the plants could still be seen from the top of a truck or a double-decker bus.⁹⁴ The court ultimately held that society did not recognize an objective expectation of privacy from the air where the plants could be seen from a legally navigable eye level and identified as marijuana with the naked eye.⁹⁵

Leaving the door open for future questions about intrusive technology, the Supreme Court was not so convinced in their holding regarding the use of high-tech cameras during searches in *Dow*.⁹⁶ Dow operated a 2,000 acre manufacturing facility in Michigan.⁹⁷ The EPA inspected the site in 1978 and then requested yet another inspection; however, Dow denied the re-inspection request.⁹⁸ In response to the denial, the EPA hired a commercial aerial photographer to take photographs of the facility from a variety of altitudes.⁹⁹ In finding that the EPA had violated Dow's expectation of privacy, the District Court put great weight on the fact that the aerial photograph captured "a great deal more than the human eye could ever see."¹⁰⁰ Ultimately, the Supreme Court decided that the photographs were not an illegal search because "the photographs . . . [were] not so revealing of intimate details as to raise to constitutional

⁹⁴ *California v. Ciraolo*, 476 U.S. 207, 211-12 (1986).

⁹⁵ *Id.* at 213-14.

⁹⁶ *Dow*, 476 U.S. at 227.

⁹⁷ *Id.* at 229.

⁹⁸ *Id.*

⁹⁹ *Id.* at 227.

¹⁰⁰ *Id.* (quoting *Dow*, 536 F. Supp. at 1367).

concerns.”¹⁰¹ However, the Court stressed that “[i]t may well be...that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.”¹⁰² While generally technology that merely enhances the human senses has been allowed in constitutionally reasonable searches, the Court has been more hesitant to provide a blanket approval for types of technology, which are either not available to the public or that bare little resemblance to human ability.¹⁰³

One of the most recent decisions regarding technology involved a search that came from *Kyllo v. United States*, where the Supreme Court invalidated a search for marijuana plants using infrared cameras.¹⁰⁴ There, the infrared cameras were focused on a suspected marijuana grower’s house in order to find “hot spots” where halide lights (powerful lamps that produce high light output for their size) were used to produce the plant.¹⁰⁵ The Court stated that “the Government use[d] a device that [was] not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance [was] a ‘search’ and [was] presumptively unreasonable without a warrant.”¹⁰⁶ The same could be said for ALPR systems that pry into the lives of innocent people, collecting small details no human could ever collect. In fact, the infrared technology of the cameras, which operated to let the

¹⁰¹ *Dow*, 476 U.S. at 238.

¹⁰² *Id.*

¹⁰³ *Kyllo*, 533 U.S. at 40.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 29-30.

¹⁰⁶ *Id.* at 40.

police officer know that marijuana was being grown, is the same infrared technology used in cameras associated with the ALPR systems.¹⁰⁷

Given that the technology used to power the ALPR is not available to the public and that it uses advanced features to process information that no human could complete, a case challenging an arrest based on an Automatic License Plate Recognition hit might have a chance to make it to the Supreme Court. The technology is not something that is readily available to the public. It is the same technology that was found to be advanced and not available to the public in *Kyllo*.¹⁰⁸ Given the high speed at which the system processes information, it could easily be grouped into a category called “highly sophisticated surveillance equipment” which the Supreme Court announced it was leery of in *Dow*.¹⁰⁹ A defendant bringing a challenge on these grounds might be able to contend that while there is no expectation of privacy while an individual is driving on the road, there is a reasonable expectation of privacy, or expectation of anonymity, while driving on a crowded freeway where a human could not possibly process all the license plates that passed at a high rate of speed. New technologies which allow police to do just that would be a violation of that reasonable expectation of privacy.

REGARDLESS OF THE QUESTIONABLE CONSTITUTIONALITY OF THE USE OF THESE AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS, THE POLICE SHOULD NOT BE ABLE TO USE THESE SORTS OF SYSTEMS WITHOUT PROPER CHECKS AND BALANCES

It is clear that Automatic License Plate Recognition systems give new power to the police. It is not only the power to instantly identify stolen cars and past due parking tickets; it is also the power to track the daily lives and movements of entirely innocent individuals. Thus far

¹⁰⁷ Gordon, *supra* note 2.

¹⁰⁸ *Kyllo*, 533 U.S. at 40.

¹⁰⁹ *Dow*, 476 U.S. at 238.

this power has not been checked. As of February 6, 2008, the phrase “automatic license plate recognition” has not shown up in any case or piece of legislation at either the state or federal level.¹¹⁰ Neither legislative bodies nor courts have taken any steps to restrict the police’s power to effectively track the daily movement of innocent people. This lack of checks has made at least one commentator nervous:

Wholesale surveillance is not simply a more efficient way for the police to do what they've always done. It's a new police power, one made possible with today's technology and one that will be made easier with tomorrow's. And with any new police power, we as a society need to take an active role in establishing rules governing its use. To do otherwise is to cede ever more authority to the police.¹¹¹

For one, legislators could require police officers to erase any information collected on someone determined not to be a criminal. Once the plate is scanned and comes back negative for any sort of warrant or outstanding fine, that information should be erased. “The police have no legitimate need to collect data on everyone's driving habits.”¹¹² Maintaining a database on the movements, locations and driving history of millions of drivers creates a security risk to every resident of a state employing the technology. The threat comes not only from those criminals who would hack into the database but also from those police officers who would overstep their authority and use that information to harass the innocent, or for their own personal agenda.

These ALPR systems have received virtually no academic or legal scrutiny; however, an analogous comparison would be facial recognition software, which has been examined much

¹¹⁰ A search of the exact phrase “automatic license plate recognition” on Feb. 6, 2008, failed to return any positive results while searching the following Westlaw databases: State Statutes-Annotated (ST-ANN-ALL); United States Code Annotated (USCA); and All Federal & State Cases (ALLCASES).

¹¹¹ Bruce Schneier (editorial), *City cops’ plate scanner is a license to snoop*, NEW HAVEN REGISTER, Sept. 19, 2004 available at <http://www.schneier.com/essay-057.html>.

¹¹² *Id.*

more closely.¹¹³ Facial recognition software operates on a similar scale as ALPR and many comparisons may be drawn. At the 2001 Super Bowl in Tampa, FaceTrac software scanned 72,000 football fans and identified 19 known criminals.¹¹⁴ Three years ago this software was already heavily used in the United Kingdom. At that time, an average person traveling through the streets of London would have been caught on film nearly three hundred times a day.¹¹⁵ Of the different cameras that film ordinary citizens, nearly three hundred in East London also employed facial recognition software.¹¹⁶ In the United States, in Washington, D.C., there are more than one-thousand surveillance cameras which are operated by various governmental agencies.¹¹⁷ In Chicago, there are at least two-thousand cameras operated by the police.¹¹⁸ It is clear that video surveillance and recognition software for faces and license plates are gaining in popularity for law enforcement departments across the world. As such, state legislatures around the nation need to respond in order to maintain protection for privacy and individual rights as this technology blossoms.

The justification for the facial recognition software is much the same as for ALPR. Facial recognition technology increases the chances of catching criminals while decreasing the demand of manpower on police departments, however, many of the same concerns with privacy and tracking are implicated:

¹¹³ See Brogan, *supra* note 56 at 73-74.

¹¹⁴ *Id.* at 80.

¹¹⁵ Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1185 (Spring 2006).

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 1188.

¹¹⁸ *Id.*

When the computer performs a wide area scan (or one-to-many match), it engages in a task that no police officer individually, or any police force as a whole, could achieve. It examines each face against as many as a billion faces for a match. But more importantly, it does so for no reason. A wide area scan is not looking for someone in particular; it is looking for anyone, suspicious or not, who happens to wander past. Furthermore, to the extent that the database tracks the location of faces it successfully scans, it operates as a homing device on a person's movements.¹¹⁹

Courts have generally been opposed to these sorts of systems ruling that “facial scanning systems are in no more common use by the general public than was the thermal sensing technology used in *Kyllo*.”¹²⁰ In fact, some states have started to take protections against the use of facial recognition software. A proposed Virginia law limits the use of facial recognition software to specific searches for specific people that last for a finite amount of time.¹²¹ This seems to be a reasonable compromise. It would allow the police to conduct a search that they deemed necessary in an emergency for the public good. However, wholesale approval for the technology is reserved in order to protect the individual liberties which are called into question with facial recognition and ALPR technology.

CONCLUSION

As technology advances every day without an effort by state legislatures, or legal scholars, to keep up with that advance, it is civil liberties and expectations of privacy that will be left behind. On the surface, Automatic License Plate Recognition systems appear to be a new form of constitutionally keeping police departments one step ahead of the criminals. While the benefits to this system are plentiful, it is important to weigh both sides of the issue and think

¹¹⁹ Brogan, *supra* note 56, at 85.

¹²⁰ *Id.* at 84.

¹²¹ Marc Jonathon Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX.L. REV. 1349, 1466 (2004). The Virginia House passed the measure, but the Virginia Senate rejected it.

critically about the impact that system will have. It is especially important to consider the privacy implications affected by this technology. Never before has this country been faced with technology of this scope. The system appears constitutional on its face, but courts must examine the system and decide whether the scope and speed at which the system processes information complies with our Constitutional expectations of privacy. While the technology ultimately presents an exciting new tool for law enforcement, it is important for lawmakers to realize the impact that this system will have on privacy rights around the country.