Rutgers University

From the SelectedWorks of Sam Hanna

Fall 2014

Orwellian Surveillance of Vehicular Travels

Sam Hanna
# Orwellian Surveillance of Vehicular Travels

By: Sam F. Hanna

## Contents

I. INTRODUCTION: ................................................................. 2  
   A. Observational Comparison: Searching Police “Hotlists”......... 3  
   B. Geolocation Memory: Recording a Vehicle’s Past Locations ...... 5  

II. BACKGROUND: ........................................................................ 8  
    A. Whether entering a license plate number into an electronic law enforcement database to obtain information constitutes a Fourth Amendment search. ..................................................... 8  

III. DISCUSSION ........................................................................... 16  
    A. Whether geolocation information that reveals a vehicle’s past location and travels is private information protected by the Fourth Amendment. ................................................................. 16  
    B. Why governmental use of ALPR to accrue and retrieve prolonged geolocation information on vehicle movements should be held unconstitutional by the Supreme Court. ................................. 25  
    C. The need for legislative intervention........................................ 34  

IV. CONCLUSION: .......................................................................... 39
I. INTRODUCTION:

“[T]here is something ‘creepy’ about continuous surveillance by the government . . . . [It is] easy to envision the worst-case Orwellian society, where all citizens are monitored by the Big Brother government.”

“Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.”

What would someone learn about you if all your automobile travels were ubiquitously tracked beginning today? Creating an indefinite database of an individual’s previous automobile travels to formulate deductions on intimate details of that person’s life is precisely what law enforcement agencies are currently able to accomplish with automatic license plate recognition technology (“ALPR”). ALPR consists of digital cameras mounted on a police cruiser that photograph the license plate numbers of passing vehicles. These cameras are linked to a computer system inside the police cruiser that convert the images of the license plate numbers into text the computer is

2 United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).
3 See discussion infra Part I.B and accompanying notes.
able to read.\textsuperscript{5} After this process occurs, the ALPR software uses a license plate number to: (a) detect whether the vehicle or its registered owner are tied to any unlawful conduct, and/or (b) produce a history on the automobile’s previous locations. These two distinct features of ALPR are discussed respectively below.

\textbf{A. Observational Comparison: Searching Police “Hotlists”}

The first method, known as the “observational comparison” feature, enters the license plate number into various law enforcement criminal databases, or “hot lists,” and ascertains the vehicle’s registered owner.\textsuperscript{6} This feature searches police hot lists to flag suspected drivers whenever a vehicle’s owner or license plate number is linked to criminal activity.\textsuperscript{7} For instance, police hot lists are used to: detect drivers with suspended licenses;\textsuperscript{8} active arrest warrants or criminal

\begin{itemize}
\item \textsuperscript{5} Id.
\item \textsuperscript{6} Rushin, supra note 3, at 283.
\item \textsuperscript{7} Norm Gaumont & Dave Babineau, The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia, POLICE CHIEF MAGAZINE, (Nov. 11, 2008) http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&amp;article_id=1671.
\item \textsuperscript{8} Tucker Mitchell, Readers utilize database to provide fast feedback on vehicles, SCNow (May 20, 2012 12:04 AM),
\end{itemize}

3 Hanna
convictions; detect unregistered vehicles and cars with stolen license plates;\(^9\) find missing persons\(^10\) and stolen cars;\(^11\) and virtually any other offense in which a license plate number or a person’s name can be used to search a law enforcement hotlist. Hence, when used in this manner, ALPR is narrowly tailored to only flag suspicious individuals and will only display data on license plates that match known or suspected individuals in criminal databases.\(^{12}\) Furthermore, because the most advanced automatic license plate readers can capture up to 1,800 license plate numbers per minute at a speed of up to 140 miles per

\(^9\) Id.
\(^{12}\) Rushin, supra note 3, at 283.
hour,\textsuperscript{13} ALPR’s observational comparison feature greatly increases the efficiency in which police can execute such tasks.

**B. Geolocation Memory: Recording a Vehicle’s Past Locations**

Secondly, the ALPR software is equipped with a “geolocation memory” feature, which is a database that saves all the previous locations any vehicle has been photographed by ALPR cameras. Each time a vehicle encounters a police vehicle equipped with ALPR technology, the ALPR software records the time, date, and global positioning system coordinates (hereinafter collectively referred to as “geolocation information” or “geolocation memory”) of where the vehicle was located when its license plate number was photographed by ALPR cameras.\textsuperscript{14} When this geolocation information is collected and saved over time, the police can use


it to trace an individual’s past automobile travels.\textsuperscript{15} Law enforcement agencies have employed the geolocation memory feature of ALPR to: solve murders and apprehend suspects;\textsuperscript{16} solve drug-related offenses;\textsuperscript{17} investigate bank robberies;\textsuperscript{18} and more.

\textsuperscript{15} See, e.g., ALPR Demo Video, MVTRAC.COM, http://mvtrac.com/alpr/demo-video/ (last visited November 19, 2012); Barbara Livingston Nackman, License plate scanner helps nab vandalism suspects, ELSAG, (April 7, 2012, 1:30 PM), http://www.elsag.com/detail.asp?i=411. For example, by utilizing this GPS locating feature, the police apprehended two suspects on felony mischief charges after a patrol car’s ALPR system produced the plate number of a vehicle that was tracked in the same area and time that the vandalism incident occurred. After analyzing the ALPR data, the police officers apprehended the suspects, who later admitted to involvement in the crime. \textit{Id.}


\textsuperscript{17} Dave Miller, Crisp deputies seize $100,000 in drug money, WALB NEWS 10 (March 5, 2012, 2:08 PM), http://www.walb.com/story/17082320/crisp-deputies-turn-suspects-over-the-dea.
However, despite the crime solving benefits associated with ALPR’s geolocation memory feature, there is a significant constitutional issue implicated when government agencies compile months or years-worth of vehicle tracking data on individuals not suspected of any criminal activity. Because ALPR systems can retain geolocation information indefinitely, it is possible for a network of ALPR cameras to facilitate mass surveillance to yield substantially intrusive personal information. This data can be highly indicative of people's lives and habits and, once it is amassed in large quantities, it is possible to decipher what people do, when they do it, and who they do it with.

This note will first provide a background on the prevailing law regarding whether running a computer check on a license plate number constitutes a Fourth Amendment search. Then, this

---

18 Mitchel Maddux, Heroin addict known as ‘Holiday Bandit’ admits to 2010 bank heists, sentenced to 15 years, NEW YORK POST, (March 14, 2012, 12:38 PM)
http://www.nypost.com/p/news/local/herion_addict_known_senteced_holiday_a0v3P62F8IWWNkC87NFF6O.

19 ACLU Seeks Details on Automatic License Plate Readers in Massive Nationwide Request, ACLU OF MARYLAND (July 30, 2012),

20 See infra Part II.B.
note will closely analyze past and current jurisprudence regarding the constitutionality and public policy concerns implicated when police use global positioning devices to monitor an individual’s automobile travels over a prolonged period of time.\textsuperscript{21} The prominence of this note will be to analyze why the Supreme Court, in light of the concurring opinions of Justice Sotomayor and Justice Alito in \textit{United States v. Jones},\textsuperscript{22} is likely to hold that long term accrual of ALPR geolocation information, without a valid search warrant, is a violation of the Fourth Amendment.\textsuperscript{23} Finally, the conclusion will: evaluate proposed legislation intended to limit the access of geolocation information; weigh the crime solving benefits of ALPR against the privacy costs; and submit a solution to retain the benefits of this technology while minimizing the costs.\textsuperscript{24}

\textbf{II. BACKGROUND:}

\textbf{A. Whether entering a license plate number into an electronic law enforcement database to obtain information constitutes a Fourth Amendment search.}

The Fourth Amendment provides “[t]he right of the people to be secure in their persons, houses, papers, and effects, against

\textsuperscript{21} See \textit{infra} Part III.A.

\textsuperscript{22} \textit{United States v. Jones}, 132 S.Ct. 945 (2012).

\textsuperscript{23} See \textit{infra} Part III.B.

\textsuperscript{24} See \textit{infra} Part IV.
unreasonable searches and seizures, shall not be violated . . . .’’25 Katz v. United States is the seminal United States Supreme Court case that established the modern two prong test for determining whether a person has constitutional protection against a government search.26 There, Justice Harlan, in a concurring opinion, delivered the settled doctrine that an individual has a Fourth Amendment privacy right against a government search of their person or things when “a person [has] exhibited an actual (subjective) expectation of privacy and . . . the expectation [is] one that society is prepared to recognize as reasonable.”27 For example, in Katz, the Supreme Court found that a person who enters a public telephone booth and shuts the door behind him exhibits a subjective and reasonable objective expectation that his conversation inside will not be intercepted by a recording device attached to the booth and overheard by government officials without his knowledge or consent.28

Unlike a conversation had in a closed phone booth, however, a more uncertain issue is whether a person possesses a subjective and objective expectation of privacy in the

25 U.S. CONST. amend. IV.
27 Id. at 361 (internal quotations omitted).
28 Id.
information that can be discovered about him by entering his vehicle’s license plate number into an electronic law enforcement database. Consideration of the following cases should provide illuminating instructing on the issue.

In United States v. Ellison, an officer noticed an occupied vehicle was idling in an area marked with “Fire Lane” and “No Parking” signs. The officer entered the vehicle's plate number into his patrol car's Law Enforcement Information Network (LEIN) and discovered the vehicle’s registered owner, Curtis Ellison, had an outstanding felony arrest warrant. The passenger, Ellison, identified himself to the officer as the vehicle’s registered owner. After notifying him of the warrant, the officer ordered Ellison to exit the vehicle and placed him under arrest. Incident to a lawful arrest, the officer patted down Ellison and discovered two firearms on his possession. Ellison was indicted for being a felon in possession of a firearm.

---

29 United States v. Ellison, 462 F.3d 557, 559 (6th Cir. 2006).

30 Id.

31 Id.

32 Id.

33 Id.

34 Id.
At trial, the district court treated the LEIN computer search on Ellison’s vehicle as a Fourth Amendment search and required the police to demonstrate probable cause to sustain the constitutionality of the search. The court held that, because the car, as a factual matter, was not parked illegally, Ellison was not engaged in any unlawful activity known to the officer. As such, the officer did not have probable cause of unlawful conduct to run the LEIN search on Ellison's license plate. Accordingly, the district court suppressed the firearms from evidence as being the fruit of an unconstitutional search.

In a 2-1 decision, however, the Sixth Circuit Court of Appeals reversed the district court, reasoning that the “[LEIN] technology used in this case does not allow officers to access any previously-unobtainable information; it simply allows them to access information more quickly.” In other words, using a license plate number to discover the outstanding felony arrest warrant does not constitute a Fourth Amendment search, which would require establishing probable cause of unlawful conduct,

---

35 Id.
36 Id.
37 Id.
38 Id.
39 Id.
because the warrant is “non-private” information. 40 Hence, discovery of the outstanding warrant by the LEIN check, which instigated the officer’s pat down search of Ellison and ultimately produced the firearms, was constitutionally valid.

However, the majority in Ellison, as Judge Karen Nelson Moore skeptically pointed out in her dissent, left open the question of how it would rule had the police used the LEIN database to obtain private information on the defendant. In light of this, Judge Moore meticulously posed this issue:

> even if there is no privacy interest in the license-plate number per se, can the police, without any measure of heightened suspicion or other constraint on their discretion, conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion? 41

By failing to address this question, the dissent criticized the majority for “pay[ing] short shrift to the crucial issue of how the license-plate information is used.” 42 Because “there [was] minimal evidence in the record and no explanation in the briefs as to what information is available from the LEIN search,” 43 Judge Moore disapproved with how the opinion of the “majority

40 Id. at 562.

41 Id. at 567.

42 Id.

43 Id.
simply presumes, without any analysis or citation to authority, that the information that is accessible through a LEIN search is otherwise available to the police without any heightened suspicion.”44 Consequently, “[t]his approach misses the crux of the issue before the court.”45

In State v. Donis, the New Jersey Supreme Court delivered a decision directly addressing and resolving the question posed by Judge Moore’s dissent in Ellison.46 In Donis, a police officer, for “no articulable reason,” entered the plate number of a vehicle traveling ahead of him into a mobile data terminal (MDT) device in his police vehicle.47 The MDT check revealed the vehicle’s registered owner had a suspended license.48 The MDT database also provided a variety of information on the vehicle’s owner defined as “personal information” under a state statute.49

Pursuant to N.J.S.A. 39:2-3.3:

“Personal information” means information that identifies an individual, including an individual's photograph; social security number; driver identification number; name; address other

44 Id. at 571.
45 Id.
47 Id. at 62.
48 Id. at 48.
49 Id.
than the five-digit zip code; telephone number; and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.\textsuperscript{50}

The Donis Court sought to “protect[] motorists from unnecessary disclosure of their personal information.”\textsuperscript{51} In doing so, the court required the MDT software to be reprogrammed so that, whenever officers use it indiscriminately without reasonable suspicion or probable cause, the device would provide only public records displaying: the registration status of the vehicle; license status of the registered owner; and whether the vehicle was reported stolen.\textsuperscript{52} Only if “the original [MDT] inquiry disclosed a basis for further police action, then the police officer would proceed to the second step, which would allow access to the ‘personal information’ of the registered owner.”\textsuperscript{53} Thus, “[w]ith the reprogrammed MDTs, police officers who were using MDTs at random and who lacked suspicion [of unlawful activity] could access only non-private information.”\textsuperscript{54}


\textsuperscript{51} Donis, 157 N.J. at 55.

\textsuperscript{52} Id.

\textsuperscript{53} Id.

\textsuperscript{54} Id. at 56.
In light of Ellison and Donis, there is a solid foundation to evaluate whether government use of ALPR’s geolocation feature is constitutional. To violate the Fourth Amendment, a record revealing a vehicle’s location and travel history must be regarded as private information.\textsuperscript{55} If so, then using ALPR to store and view this information, without establishing reasonable suspicion or probable cause, is an unconstitutional search in violation of the Fourth Amendment.\textsuperscript{56} In contrast, if one’s automobile location and travels is regarded as public knowledge, then use of ALPR technology by the government to view this

\textsuperscript{55} In addition to collecting and saving GPS locating information, ALPR analyzes several databases that produce multiple piece of information, which “when merged, can also be personally identifiable, even where each individual piece of data itself would not.” International Association of Chiefs of Police, Privacy impact assessment report for the utilization of license plate readers, 6, (2009), available at http://www.theiACP.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87. However, this note only emphasizes the privacy concerns implicated by collecting GPS data.

\textsuperscript{56} See, e.g., Donis, 157 N.J. 44.
information is afforded no protection because it would not constitute a search within the meaning of the Fourth Amendment.\textsuperscript{57}

III. DISCUSSION

A. Whether geolocation information that reveals a vehicle’s past location and travels is private information protected by the Fourth Amendment.

In \textit{United States v. Knotts}, the United States Supreme Court considered for the first time whether the use of a tracking device constitutes a Fourth Amendment “search.”\textsuperscript{58} In Knotts, the Supreme Court held that using a beeper to monitor the movements of a third person, which ultimately led police to the defendant’s drug lab, did not amount to a search.\textsuperscript{59} First, the Court applied the two-prong \textit{Katz} test and determined that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy from one place to another.”\textsuperscript{60} Consequently, the Court refused to find that defendant’s Fourth Amendment right was violated by using the beeper to track his location because the “beeper surveillance amounted principally

\begin{footnotesize}
\begin{itemize}
\item[57] See, e.g., Ellison, 462 F.3d 557.
\item[59] Id. at 285.
\item[60] Id.
\end{itemize}
\end{footnotesize}
to [nothing more than] the following of an automobile on public streets and highways."\(^{61}\)

In *Knotts*, defendant’s counsel argued that failing to recognize the use of a tracking device as a search would amount to “twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision.”\(^{62}\) The Court was unmoved by this public policy concern because the specific circumstances before it “hardly suggest abuse.”\(^{63}\) In *Knotts*, the beeper only tracked a relatively brief trip, which was easily and equally achievable without use of the beeper through traditional law enforcement surveillance methods. Therefore, the Court, with three separate concurring opinions, upheld the constitutionality of the vehicular tracking in this case.\(^{64}\)

Nonetheless, the *Knotts* Court, looking forward, noted that “if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough

\(^{61} Id.\.

\(^{62} Id.\) at 283.

\(^{63} Id.\) (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 566 (1978)).

\(^{64} Id.\) at 284.
then to determine whether different constitutional principles may be applicable.”

Those “dragnet type law enforcement practices” were used in United States v. Maynard, where the District of Columbia Court of Appeals circumstantially narrowed the applicability of Knotts. In Maynard, the police installed a GPS tracking device on defendant’s vehicle to track his movements twenty four hours per day for twenty eight days. Using the data, the state established a travel pattern consistent with drug trafficking. Applying Katz, the court explained that “[i]n considering whether something is ‘exposed’ to the public . . . we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.” Consequently, the court found that defendant had a reasonable expectation his vehicle would not be tracked over the course of a month because “the likelihood a stranger would observe all those movements is not just remote, it is

---

65 Id. at 284.

66 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

67 Id. at 567.

68 Id.

69 Id. at 559 (emphasis added).
essentially nil.”  

In addition, the *Maynard* court convincingly distinguished the prolonged GPS tracking that took place here from the single and brief journey monitored in *Knotts* because:

> prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Accordingly, the *Maynard* court held that the month long surveillance of defendant's vehicle produced private information, thereby constituting an unreasonable “search.”

In contrast, *United States v. Sparks* utilized a substantially different analytical approach than *Maynard*.

---

70 Id. at 560.

71 Id. at 562.

72 Id. at 564.
There, the FBI installed a GPS device on defendant’s vehicle because they suspected he had committed three bank robberies in the preceding three months.\textsuperscript{74} Eleven days later, a bank robbery occurred and nearby police observed two men wearing dark clothing and carrying a brown bag enter the defendant’s vehicle.\textsuperscript{75} After losing physical sight of the vehicle, investigators used the GPS tracking device to reacquire visual surveillance on the car and initiate a traffic stop.\textsuperscript{76} After pulling over, the occupants, still unidentified at this time, exited the car and escaped into the nearby woods.\textsuperscript{77} The agents examined the GPS tracking data and discovered that, on the day of the robbery, the vehicle traveled from the defendant’s apartment to the street where police observed the suspected robbers enter the vehicle.\textsuperscript{78} The defendant moved to suppress all the tracking evidence ascertained by way of the GPS device.\textsuperscript{79}

\textsuperscript{73} United States v. Sparks, 750 F.Supp.2d 384 (Mass. Dist. Ct. 2010).
\textsuperscript{74} Id. at 387.
\textsuperscript{75} Id. at 386.
\textsuperscript{76} Id.
\textsuperscript{77} Id.
\textsuperscript{78} Id.
\textsuperscript{79} Id. at 387.
Ruling on defendant’s suppression motion, Judge William Young not only rejected the Maynard analysis, but adopted completely contrary legal principles. As discussed earlier, in determining whether tracking data is private information, the Maynard court: (1) considered the probability that a stranger would observe all of one’s travels over the span of time\(^80\) and (2) held that the aggregate of one’s travels are more private than travels viewed in isolation.\(^81\) In contrast, Sparks: (1) considered “not what a random stranger would actually or likely do, but rather what he feasibly could [do]”\(^82\) and (2) held that “[a]lthough [] continuous monitoring may capture quantitatively more information than brief stints of surveillance, the type of information collected is qualitatively the same.”\(^83\) Hence, the Sparks factors are directly contrary to the Maynard factors. Judge Young criticized Maynard as being “vague and unworkable” because “conduct that is initially constitutionally sound could later be deemed impermissible if it becomes part of the aggregate.” Consequently, “[i]t is unclear when surveillance becomes so prolonged as to have crossed the threshold and

\(^80\) Maynard, 615 F.3d at 560.

\(^81\) Id. at 562.

\(^82\) Sparks, 750 F.Supp.2d at 391 [emphasis added].

\(^83\) Id. at 392.
created this allegedly intrusive mosaic.” Accordingly, the court held that “Sparks's argument, that the aggregate of his travels are entitled to more constitutional protection than his individual trips, must fail.”

Despite this seemingly hostile holding, Judge Young conceded in dicta that “the use of the GPS device on Sparks's vehicle is more akin to the use of the beeper in Knotts than that of the GPS device in Maynard.” This is because the GPS device in Sparks, like the beeper in Knotts, was used for a brief time and for the limited purpose of conducting and ascertaining visual surveillance. In contrast, the device in Maynard was used to conduct a month-long, twenty-four hour surveillance on the defendant, intended to elucidate a picture of his life and habits. Though Sparks initially appeared unreceptive to the distinction between short term and long term GPS tracking, the court conceded in dicta that it “is not unsympathetic to the sentiment . . . that there is something ‘creepy’ about continuous surveillance by the government . . . . [It is] easy to envision the worst-case Orwellian society, where

---

84 Id. at 393.
85 Id. at 395.
86 Maynard, 615 F.3d at 560.
all citizens are monitored by the Big Brother government.”^{87} Despite these concerns, much like the rebuttal in *Knotts*,^{88} *Sparks* refused to address this latter issue, because such practices “have yet to materialize, and are certainly not at issue in this case.”^{89}

Three years before *Sparks*, the Seventh Circuit similarly recognized the privacy implications raised by mass governmental tracking of a vehicle’s movement.^{90} In *United States v. Garcia*, Judge Posner envisioned how:

> [o]ne can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. One can even imagine a law requiring all new cars to come equipped with the device so that the government can keep track of all vehicular movement in the United States. It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment . . . . Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.”^{91}

^{87} *Sparks*, 750 F.Supp.2d at 395.

^{88} *Knotts*, 460 U.S. at 284

^{89} *Id.* at 396.

^{90} *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007).

^{91} *Id.* at 998 (emphasis added).

23 Hanna
The advent of ALPR technology makes learning the past and present location of thousands, or even millions, of vehicles completely possible and easily achievable by the government.\textsuperscript{92} As of 2009, police departments nationwide have increasingly affixed ALPR cameras to their police cruisers.\textsuperscript{93} In addition to the mobile ALPR devices, stationary ALPR cameras can be installed on street signs, street lights, highway overpasses, buildings, and so on to photograph passing automobiles and, thus, keep an indefinite record of each time any vehicle travels past that


\textsuperscript{93} Lum, Merola, Willis, and Cave, License plate recognition technologies for law enforcement: An outcome and legitimacy evaluation. For example, a September 2009 national survey found that 37% of agencies with greater than 100 officers already use ALPR technology and that nearly one-third of the remaining agencies surveyed planned to acquire it within one year. \textit{Id.}
stationary point. Installing enough of these fixed cameras strategically in a community, combined with the tracking information collected from mobile devices on police cruisers, can comprehensively facilitate mass surveillance of the vehicular travels of an entire community. Moreover, because ALPR is capable of retaining this geolocation tracking data indefinitely for subsequent observation, police can use the device’s memory to observe past travels and, hence, predict future movements of any vehicle, deduce intimate details of a person’s life and relationships, and learn many of a person’s daily routine and habits. The unbridled and unregulated use of this tool advances the same “dragnet type [of] law enforcement practices” fictionalized by Knotts and makes the “worst-case


95 Rushin, supra note 3, at 283.


97 See supra note 66 and accompanying text.
Orwellian society” feared of by Sparks\textsuperscript{98} wholly feasible. Allowing the government to implement the use of ALPR in this way threatens fundamental Fourth Amendment values and dismantles historically accepted expectations of privacy.

**B. Why governmental use of ALPR to accrue and retrieve prolonged geolocation information on vehicle movements should be held unconstitutional by the Supreme Court.**

It is imperative that the Supreme Court finally determine the constitutionality of compiling the vehicular travel history and present locations of individuals not suspected of unlawful activity. *United States v. Jones*, a companion case of *Maynard*,\textsuperscript{99} *supra*, is the most recent Supreme Court case likely to provide guiding federal precedent on this issue.\textsuperscript{100} In *Jones*, the FBI procured a search warrant authorizing the installation of a tracking device on the defendant’s vehicle.\textsuperscript{101} However, the FBI agents installed the device on the vehicle a day after the warrant expired and outside of the issuing court's jurisdiction, rendering it invalid.\textsuperscript{102} Nonetheless, over the next 28 days, the

\textsuperscript{98} See *supra* note 87 and accompanying text.

\textsuperscript{99} *Maynard*, 615 F.3d 544. See *supra* notes 66-72 and accompanying text.

\textsuperscript{100} United States v. Jones, 132 S.Ct. 945 (2012).

\textsuperscript{101} *Id.*

\textsuperscript{102} *Id.*
device produced over 2,000 pages of data tracking the vehicle’s movements, which connected defendant to an alleged conspirators' stash house that contained $850,000 in currency and 97 kilograms of cocaine.\textsuperscript{103} Jones motioned to suppress all evidence obtained in violation of the Fourth Amendment.\textsuperscript{104} As mentioned in the Maynard discussion, supra,\textsuperscript{105} the District of Columbia Court of Appeals ruled in favor of Jones and Maynard, co-conspirators, finding that the nearly month long tracking of his vehicle was unconstitutional absent a valid search warrant.\textsuperscript{106}

The Supreme Court of the United States granted certiorari to determine the Fourth Amendment issue.\textsuperscript{107} Though the Supreme Court found that the government’s warrantless actions in Jones amounted to a search, it did so by applying antiquated common law trespass jurisprudence, rather than the Katz expectation of privacy test, supra.\textsuperscript{108} Justice Scalia, writing for the Court, focused on the fact that, by installing the GPS tracking device on the undercarriage of defendant’s vehicle, the government

\begin{itemize}
    \item \textsuperscript{103} Id. at 948-49.
    \item \textsuperscript{104} Id.
    \item \textsuperscript{105} See supra notes 66-72 and accompanying text.
    \item \textsuperscript{106} Maynard, 615 F.3d at 564.
    \item \textsuperscript{107} Jones, 132 S.Ct. 945.
    \item \textsuperscript{108} Id. at 949. See also supra notes 25-28 and accompanying text.
\end{itemize}
trespassed on defendant’s property.\textsuperscript{109} According to Justice Scalia, this conduct amounted to “physically occup[ying] private property for the purpose of obtaining information.”\textsuperscript{110} Consequently, because “such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted,” Justice Scalia held that “the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a ‘search.’”\textsuperscript{111} By deciding the case using trespass jurisprudence, which was applicable before the Katz test, Justice Scalia did not overturn the Katz test, but merely wanted to clarify that “the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”\textsuperscript{112}

In essence, instead of holding that the prolonged tracking of a vehicle’s travels is unconstitutional because it violates a reasonable expectation of privacy, Justice Scalia merely made it unlawful for the government to physically install a tracking device on one’s property without a valid warrant.\textsuperscript{113} This

\begin{footnotes}
\item[109] Id.
\item[110] Id.
\item[111] Id.
\item[112] Id. at 952.
\item[113] Id.
\end{footnotes}
holding, however, provides the government a loophole to accomplish the same evil. For instance, what if the police did not affix a GPS tracking device on defendant’s vehicle and were able to track his automobile travels using a more sophisticated tracking method (i.e., ALPR cameras)? Pursuant to Justice Scalia’s opinion, this tech savvy method of tracking one’s automobile travels would be permissible under Jones because it does not require a physical trespass on the vehicle. This loophole renders Justice Scalia’s holding inexcusably shortsighted and incapable of protecting against modern methods of government surveillance. If the same end (compiling weeks-worth of tracking data on a person’s automobile travels) is achievable using a more technologically advanced means, should the mere absence of a physical trespass to obtain the same information be the determinative factor of whether one may assert a violation of his Fourth Amendment right to privacy?

To answer this, consider why the Supreme Court, in Katz v. United States, transcended the trespassory test in favor of adopting the modern expectation of privacy test. The Katz test provides Fourth Amendment protection based on “a legitimate

expectation of privacy in the invaded space,”\textsuperscript{115} not merely on “the presence or absence of a physical intrusion into any given enclosure.”\textsuperscript{116} If Katz did not transcend the trespassory test, the Court would not have found a search occurred when the government placed a recording device on the outside of a telephone booth because the booth did not belong to the defendant and, thus, there could not be a showing of trespass on private property.\textsuperscript{117} However, the Court recognized that placing the recording device on the booth to replay a person’s telephone conversation violated an expectation of privacy that most individuals expect existed in the booth, and this expectation is what the Court believed ought to be protected by the Fourth Amendment, not the existence or absence of a physical

\textsuperscript{115} Rakas v. Illinois, 439 U.S. 128, 143 (1978) (“[The] capacity to claim the protection for the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.”); see also Katz, 389 U.S. at 353 (“The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.”).

\textsuperscript{116} Katz, 389 U.S. at 353.

\textsuperscript{117} See id.
trespass.\textsuperscript{118} The Court explained, “once it is recognized that the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.”\textsuperscript{119}

Accounting for these concerns, Justice Alito criticized Justice Scalia’s opinion as being “unwise” and “highly artificial” for applying “18\textsuperscript{th} century tort law” to a “21\textsuperscript{st}-century surveillance technique.”\textsuperscript{120} Justice Alito recognized:

the Court’s reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car’s operation).\textsuperscript{121}

In light of this deficiency, Justice Alito believed that the question presented in Jones should be answered by applying the Katz test to determine whether defendant’s reasonable

\textsuperscript{118} See id.

\textsuperscript{119} Id.


\textsuperscript{121} Id. at 961.
expectation of privacy was violated by the four week government surveillance of his vehicle’s movements.\(^\text{122}\) Accordingly,

\[
\text{[u]nder this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.}\(^\text{123}\)
\]

Justice Sotomayor, in a separate concurring opinion, illuminated why long term government surveillance of vehicular travels violates a reasonable expectation of privacy.\(^\text{124}\) Like several other courts,\(^\text{125}\) Justice Sotomayor noted that “GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”\(^\text{126}\) For instance:

\(^{122}\) Id. at 958.

\(^{123}\) Id. at 964.

\(^{124}\) Id. at 954-57.

\(^{125}\) See, e.g., Maynard, 615 F.3d at 562; Zahn, 812 N.W.2d at 497; Garcia, 474 F.3d at 998; and People v. Weaver, 882 N.Y.S.2d 357, 361 (N.Y. 2009).

\(^{126}\) Jones, 132 S.Ct. at 956.
[d]isclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.\textsuperscript{127} This information is even more intrusive when “[t]he Government can store such records and efficiently mine them for information years into the future.”\textsuperscript{128} Hence, Justice Sotomayor opined that long term tracking of a person’s vehicular travels breaches an expectation of privacy the Fourth Amendment exists to protect.\textsuperscript{129}

In sum, the concurring opinions of Justice Alito and Sotomayor provide two persuasive reasons why Justice Scalia’s decision to apply the trespassory test undermines modern-day surveillance methods. First, the “trespassory test may provide little guidance” to “novel modes of surveillance that do not depend upon a physical invasion on property.”\textsuperscript{130} Second, because “the Fourth Amendment protects people, not places,”\textsuperscript{131} the appropriate test should be to “ask whether people reasonably

\begin{flushright}
\textsuperscript{127} \textit{Id.}
\end{flushright}

\begin{flushright}
\textsuperscript{128} \textit{Jones}, 132 S.Ct. at 955-56.
\end{flushright}

\begin{flushright}
\textsuperscript{129} \textit{Id.} at 955.
\end{flushright}

\begin{flushright}
\textsuperscript{130} \textit{Id.}
\end{flushright}

\begin{flushright}
\textsuperscript{131} \textit{Katz}, 389 U.S. at 351.
\end{flushright}
expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. 132 Justices Alito and Sotomayor have already answered in the negative. 133

Understanding how the nine Justices voted in Jones provides insight on how each would vote in respect to whether using ALPR technology to track a vehicle’s location is lawful. Chief Justice Roberts and Justices Kennedy, Thomas and Sotomayor joined Justice Scalia’s opinion, making it the majority. 134 However, had Justice Sotomayor joined Alito’s concurrence instead, then Justice Alito’s opinion would constitute the majority because Justices Ginsburg, Breyer, and Kagan all joined. 135 Nonetheless, the concurrences of Justice Alito and Sotomayor command five votes. Consequently, this means that a potential majority of the current members of the Supreme Court, not only advocate the Katz test but, believe that long term monitoring of one’s travels impinges on a reasonable expectation of privacy, thereby constituting a Fourth Amendment violation.

132 Jones, 132 S.Ct. at 955.
133 Id. at 955, 964.
134 Id. at 947.
135 Id. at 957.
C. The need for legislative intervention.

Nonetheless, though at least five Supreme Court Justices appear to agree that tracking one’s automobile travels for four weeks constitutes a search, there is no reason to wait until the constitutional issue reaches the Court again. The United States Constitution sets the minimal protections against government agents, but state or federal legislatures are free to expand protection to privacy and property. In several ways, the legislature is perhaps even more capable at achieving this purpose than the judiciary when technology threatens privacy. “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”\textsuperscript{136}

Despite the potentially devastating effects to individual privacy that would result if ALPR devices become a ubiquitous presence in our communities, the solution is straightforward: impose legislative restrictions on the collection, storage, and dissemination of vehicular geolocation data. However, for the legislation to be effective, it is essential that it balance two distinct competing interests. The legislation must be

\textsuperscript{136} Id. at 964.
meticulously crafted to: (1) permit law enforcement to employ
ALPR devices for its valuable crime solving capabilities (i.e.,
observational comparison) and (2) draw effective boundaries to
ensure it is not used as a tool for conducting indiscriminate
and ubiquitous surveillance.

Considering the drastic difference a poorly versus well
drafted statute can have,\textsuperscript{137} Congress should take the initiative
to craft federal legislation that will properly balance the
competing private and public policy concerns. Because there is
currently federal legislation regulating the use of privacy
threatening technology,\textsuperscript{138} Congress is very likely within its
legislative capacity to regulate the use of ALPR devices. For
instance, the Electronic Communications Privacy Act is a federal
law that currently governs the use of wiretapping and electronic
eavesdropping.\textsuperscript{139} Senator Patrick Leahy proposed an amendment to
this Act, entitled the Electronic Communications Privacy
Amendments Act of 2011 (ECPAA), which provides that, unless a
warrant based upon probable cause is obtained, “no governmental
entity may access or use an electronic communications device to


\textsuperscript{138} See, e.g., 18 USCA § 251.

\textsuperscript{139} Id.
acquire geolocation information." If enacted, the ECPAA bill would greatly circumscribe law enforcement’s ability to use ALPR’s geolocation memory feature and, thus, prevent this device from being used indiscriminately by police as a tool for mass surveillance of vehicular travels.

As mentioned, the ECPAA permits the government to use a geolocation acquiring device only upon procurement of a search warrant based upon probable cause. However, an exigency exception to the search warrant requirement exists if there are grounds to believe that a search warrant could be obtained, but the acquisition of a warrant is made impracticable due to an emergency that involves: (a) immediate danger of death or serious bodily injury to any person; (b) conspiratorial activities illustrative of organized crime; or (c) an immediate threat to national security. Nonetheless, this warrant exception is limited because, “not later than 48 hours after the


142 S. 1011, 112th Cong., 1st Sess, 18 USC § 2713(d)(1).
activity to acquire the geolocation information has occurred,” the government must seek a warrant. If a warrant is not obtained, use of the device to acquire geolocation information must terminate immediately once the earlier of any of the following occur: (a) the information sought is obtained; (b) the application for the warrant is denied; or (c) 48 hours have elapsed since the activity to acquire the geolocation information commenced. If the government fails to comply with these provisions, no information or evidence derived from the use of a geolocation information acquiring device may be entered into evidence or otherwise disclosed in any trial nor may it be disclosed in any other manner, without the person’s consent.

The ECPAA bill does several things right. It makes the unwarranted use of ALPR’s geolocation memory feature unlawful and, thus, immediately proscribes the devices current method of operation, which is a mindless, automatic collection and retention of the geolocation information of every vehicle the device captures on camera. Hence, this would ban ALPR’s use as a tool to conduct mass surveillance of vehicular movements, and thereby significantly protect privacy. Nonetheless, the ECPAA

bill’s exigency exception effectively balances law enforcement and public safety needs by permitting the device to be used without a warrant in exigent circumstances. Moreover, the exclusionary provision of the ECPAA bill will ensure that the government will not disregard the warrant requirement because any information unlawfully obtained will not be admitted into evidence, thereby giving police no incentive to capture geolocation information without authorization. Finally, because ALPR’s observational comparison feature does not acquire geolocation information, the ECPAA bill does not interfere with this aspect of the device. Thus, police may continue to employ the observational comparison feature to detect if any vehicle or its registered owner is listed in any police hotlist without the need to obtain a warrant. Hence, the ECPAA bill successfully provides the proper balance needed to level the privacy and public policy concerns associated with use of ALPR technology. Accordingly, it is in society’s best interest to advocate for and support passing this legislation.

IV. CONCLUSION:

Members of the United States Supreme Court, district and circuit courts, and state court judges around the country have all acknowledged the potentially devastating effects mass surveillance of vehicular travels can have on individual
privacy. Unaware that this threat can be implemented today, the judiciary has been presented with the opportunity, but refused, on several occasions to directly rule on the constitutionality of this issue. However, with the ubiquity of ALPR cameras, continuous government surveillance of automobile travels is no longer a figment of the imagination. Consequently, the judicial and legislative branches of government must embark on balancing the private and public interests implicated by this technology. Failure to set suitable boundaries around the use of this technology can and will significantly undercut Fourth Amendment privacy rights in this and possibly other contexts.