Spring 2015

ORWELLIAN SURVEILLANCE OF VEHICULAR TRAVELS

Sam F. Hanna

ORWELLIAN SURVEILLANCE OF VEHICULAR TRAVELS

SAM F. HANNA

In United States v. Jones,[1] *the State planted a tracking device on an individual's vehicle to track that vehicle's travels twenty-four hours per day for twenty-eight days. The Court held that, because planting the device amounted to a physical trespass on private property, this amounted to a Fourth Amendment search under the historical 'trespassory test'. However, the Court's reliance on the trespassory test fails to take account of a modern surveillance method, known as automatic license plate recognition ("ALPR"), which makes it possible to track an automobile's travels without the need to plant a tracking device on the vehicle. Consequently, by deciding the Jones case under the antiquated trespassory test, the Court's opinion is shortsighted in two material respects. First, it fails to answer the underlying legal issue of whether prolonged police surveillance of automobile travels is constitutional. Second, it provides the State a loophole to accomplish the same objective by using a different, more technologically advanced, means.*

However, is it sensible to make the absence or presence of a trespass on a vehicle the dividing line between whether or not the Fourth Amendment affords constitutional protection against automobile surveillance? In other words, should the means used to accomplish the objective dictate whether or not the constitution has been violated? Is it not more prudent to make the underlying objective itself the subject of the Court's constitutional analysis?

The purpose of this note is to answer a question that the Jones Court, and many courts nationwide, have either avoided or failed to reach a unanimous decision on – that is, do individuals possess a constitutional expectation of privacy that the State will not indiscriminately conduct prolonged mass surveillance of their automobile travels without first obtaining a valid search warrant?

[1] 132 S.Ct. 945 (2012).

INTRODUCTION

"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."[2]

Today, it is possible to create an indefinite database of the automobile travels of every person nationwide through the use of automatic license plate recognition technology ("ALPR").[3] ALPR consists of digital cameras that can be mounted ubiquitously onto either police vehicles or fixed stationary positions, including sign-posts, traffic signals, street lights and virtually any other stationary position.[4] These cameras indiscriminately photograph the license plate numbers of every vehicle within its range. Because the cameras record the date, time, and geographic coordinates of where and when a vehicle is photographed, each individual photograph can be used in conjunction with potentially hundreds, or thousands, of previous photographs to form a mosaic-like picture that reveals an individual's entire travel history.[5]

Law enforcement agencies have successfully employed ALPR to investigate crimes and apprehend suspects.[6]

However, despite the crime-solving benefits associated with ALPR, there is a significant constitutional issue implicated when government agencies compile information on an individual's automobile travels without possessing reasonable suspicion of criminal activity.

---

[2] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

[3] *See* Tyson E. Hubbard, *Automatic License Plate Recognition: An Exciting New Law Enforcement Tool with Potentially Scary Consequences,* 18 Syracuse Sci. & Tech. L. Rep. 3 (2008); Carol Robinson, *Deputies to deploy plate ID system: System compares car tags, databases to expose criminals*, BIRMINGHAM NEWS, Mar. 24, 2006, at 1C.

[4] Stephen Rushin, *The Judicial Response to Mass Police Surveillance,* 2011 U. Ill. J.L. Tech. & Pol'y 281, 285 (2011).

[5] *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.

[6] *Highway cameras help catch accused killer*, ABC News 4 (May 11, 2011, 8:37 PM), http://www.abcnews4.com/story/14629468/highway-cameras-help-catch-accused-killer; *See also* 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; *See also* 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/heroin_addict_known_senteced_holiday_a0v3P62F8IWWNkC87NFF6O.

Moreover, with the capability to retain travel history indefinitely,[7] a ubiquitous network of ALPR cameras can be used to facilitate mass surveillance of vehicular travels – a modern practice that threatens Fourth Amendment principles.

The purpose of this note is to analyze whether the State's use of ALPR to conduct mass government surveillance of automobile travels constitutes a search within the meaning of the Fourth Amendment. In doing so, this note will evaluate how district and circuit courts across the United States have historically dealt with government surveillance of automobile travels.[8] This precedential history will be useful in analyzing the Supreme Court's recent decision in *United States v. Jones.*[9] The purpose in addressing *Jones* is two-fold: (1) to point out how the Court's short-sighted reliance on the trespassory test fails to account for modern surveillance methods, such as ALPR; and, (2) to analyze each Justice's position regarding whether or not twenty-four surveillance of vehicular travels for weeks, or even months, on end violates an expectation of privacy under the *Katz* test. Finally, this note will discuss a legislative bill that addresses the Fourth Amendment issue implicated by the use of technology such as ALPR, and which proposes a solution that balances the State's interest in conducting surveillance of automobile travels for crime solving purposes, against society's interest in preserving Fourth Amendment privacy rights.[10]

I. BACKGROUND

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 . . . ."[11] *Katz v. United States* is the seminal United States Supreme Court case that established the modern two-prong test for determining whether certain government action constitutes an "unreasonable search" within the meaning of the Fourth Amendment.[12] There, Justice Harlan, in a concurring opinion, delivered the settled doctrine that an "unreasonable search" occurs when the Court finds that "a person [has] exhibited an actual (subjective) expectation of privacy and . . . the expectation [is] one that society is prepared to recognize as [objectively] reasonable."[13]

---

[7] *ACLU Seeks Details on Automatic License Plate Readers in Massive Nationwide Request*, ACLU OF MARYLAND (July 30, 2012), http://www.aclu-md.org/press_room/75.
[8] See *infra* Part III.A.
[9] United States v. Jones, 132 S.Ct. 945 (2012).
[10] See *infra* Part IV.
[11] U.S. CONST. amend. IV.
[12] Katz v. United States, 389 U.S. 347, 351 (1967).
[13] *Id*. at 361 (internal quotations omitted).

In *Katz*, the Supreme Court found that a defendant who enters a public telephone booth and shuts the door behind him exhibits a subjective and objective expectation that his conversation inside will not be overheard. Therefore, when law enforcement attached a recording device on a phone-booth to intercept a defendant's conversation without his knowledge or consent, the Supreme Court held that this government action constituted an "unreasonable search" under the Fourth Amendment.[14]

II. DISCUSSION

A. WHETHER GEOLOCATION INFORMATION THAT REVEALS A VEHICLE'S PAST LOCATION AND TRAVELS IS PRIVATE INFORMATION PROTECTED BY THE FOURTH AMENDMENT

In *United States v. Knotts,* the United States Supreme Court considered for the first time whether the use of a locational tracking device constitutes a "search," within the meaning of the Fourth Amendment.[15] 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.[16] First, the Court applied the two-prong *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."[17] 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 to [nothing more than] the following of an automobile on public streets and highways."[18]

In *Knotts,* the defendant's counsel argued that failing to recognize the use of a tracking device as a Fourth Amendment search would amount to "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision."[19] The Court was unmoved by this public policy concern because the specific factual circumstances presented in the case before it "hardly suggest abuse."[20] 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

[14] *Id*.
[15] Unites States v. Knotts, 460 U.S. 276 (1983).
[16] *Id*. at 285.
[17] *Id*.
[18] *Id*.
[19] *Id*. at 283.
[20] *Id*. (quoting Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).

methods, such as physically following the vehicle. Therefore, the Court, with three separate concurring opinions, upheld the constitutionality of the vehicular tracking device in this case.[21] Nonetheless, the *Knotts* Court, looking into the future, noted in dicta that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[22]

Those "dragnet type law enforcement practices" were employed in *United States v. Maynard*, where the District of Columbia Court of Appeals narrowed the applicability of *Knotts* when presented with a different set of facts.[23] 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.[24] Using the data, the state established a travel pattern consistent with drug trafficking.[25] 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."[26] Consequently, the court found that the 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 essentially nil."[27] In addition, the *Maynard* court distinguished the prolonged GPS tracking that took place here from the single and brief journey monitored in *Knotts*, supra, because:

> [p]rolonged 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

[21] *Id*. at 284.
[22] *Id*. at 284.
[23] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
[24] Id. at 567.
[25] *Id*.
[26] *Id*. at 559 (emphasis added).
[27] *Id*. at 560.

> 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.[28]

Accordingly, the *Maynard* court held that the month long surveillance of defendant's vehicle produced private information that the defendant had a reasonable expectation of privacy in.[29]

In contrast, *United States v. Sparks* utilized a substantially different analytical approach than *Maynard*.[30] 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.[31] Eleven days later, a bank robbery occurred and police near to the scene observed two men wearing dark clothing and carrying a brown bag enter defendant's vehicle.[32] After losing physical sight of the subject vehicle, investigators used the GPS tracking device to reacquire visual surveillance on the car and initiate a traffic stop.[33] After pulling over, the occupants, still unidentified at this time, exited the car and escaped into the nearby woods.[34] The agents examined the GPS tracking data and discovered that, on the day of the robbery, the subject vehicle traveled from the defendant's apartment to the street where police observed the suspected robbers enter the vehicle.[35] The defendant moved to suppress all the tracking evidence ascertained from the GPS device.[36]

Ruling on the defendant's suppression motion, Judge William Young not only rejected the *Maynard* analysis, but adopted completely contrary legal principles. To briefly recount, in determining whether vehicular surveillance constituted a search, the *Maynard* court: (1) considered the probability that a stranger would observe all of one's travels over the span of or a prolonged period of time[37] and (2) held the aggregate of one's travels are more private than travels viewed in isolation.[38] In contrast, *Sparks*: (1) considered "not what a random stranger would actually or likely do, but rather what he feasibly could [do]"[39] and (2) held that "[a]lthough [] continuous monitoring may capture quantitatively more information than brief stints of surveillance, the type of information

[28] *Id*. at 562.
[29] *Id*. at 564.
[30] United States v. Sparks, 750 F.Supp.2d 384 (Mass. Dist. Ct. 2010).
[31] *Id*. at 387.
[32] *Id*. at 386.
[33] *Id*.
[34] *Id*.
[35] *Id*.
[36] *Id*. at 387.
[37] *Maynard*, 615 F.3d at 560.
[38] *Id*. at 562.
[39] *Sparks*, 750 F.Supp.2d at 391 [emphasis added].

collected is qualitatively the same."[40] Accordingly, 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." Because of this, Judge Young criticized *Maynard* on grounds that "[i]t is unclear when surveillance becomes so prolonged as to have crossed the threshold and created this allegedly intrusive mosaic." Accordingly, the court held that "[defendant's] argument, that the aggregate of his travels are entitled to more constitutional protection than his individual trips, must fail."[41]

Notwithstanding his sharp criticism of *Maynard*, 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*."[42] 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.[43] Though Judge Young, in his opinion in *Sparks,* initially appeared unreceptive to the distinction between short term and long term GPS tracking, he conceded in dicta that he "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 all citizens are monitored by the Big Brother government."[44] However, despite these concerns, much like the escape taken in *Knotts*,[45] *Sparks* refused to address this latter issue, because such practices "have yet to materialize, and are certainly not at issue in this case."[46]

Three years before *Sparks*, the Seventh Circuit similarly recognized the privacy implications raised by mass governmental tracking of a vehicle's movement.[47] 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

[40] *Id*. at 392.
[41] *Id*. at 393.
[42] *Id*. at 395.
[43] *Maynard*, 615 F.3d at 560.
[44] *Sparks,* 750 F.Supp.2d at 395.
[45] *Knotts*, 460 U.S. at 284
[46] *Id*. at 396.
[47] United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

> 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.[48]

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.[49] As of 2009, police departments nationwide have increasingly affixed ALPR cameras to their police cruisers.[50] In addition to the mobile ALPR devices, stationary ALPR cameras can be installed on street signs, street lights, highway overpasses, buildings, and bridges, etc. to photograph passing automobiles and, thus, keep an indefinite record of each time any vehicle travels past those locations.[51] Installing enough of these fixed cameras strategically in a community, combined with the cameras affixed on police cruisers, can facilitate mass surveillance of virtually all automobile travels across the United States. Moreover, because ALPR is capable of retaining this tracking data indefinitely for subsequent observation,[52] police can use the device's memory to: observe past travels, predict future travels, deduce intimate details of a person's life and relationships, and learn many of a person's daily routines and habits.[53] The unbridled and unregulated use of ALPR advances the same "dragnet type [of] law enforcement practices" fictionalized by *Knotts*[54] and makes the "worst-case Orwellian society" feared of by *Sparks*[55] wholly feasible. It is easy to see how a lack of judicial oversight on the use of ALPR threatens historical Fourth Amendment values and long accepted expectations of privacy.

---

[48] Id. at 998 (emphasis added).

[49] Brian Alseth, Automated License Plate Recognition: The Newest Threat to Your Privacy When you Travel, ACLU of Wash. Blog (May 26, 2010, 9:31 AM), http://www.aclu-wa.org/blog/automated-license-plate-recognition-newest-threat-your-privacy-when-you-travel.

[50] 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. *Id*.

[51] Automatic License Plate Recognition (ALPR), WHATIS.COM, http://whatis.techtarget.com/definition/Automated-License-Plate-Recognition-ALPR (last visited March 1, 2013).

[52] Rushin, *supra* note 3, at 283.

[53] *See* ALPR Demo Video, MVTRAC.COM, http://mvtrac.com/alpr/demo-video/ (last visited November 19, 2012); Mary Beth Sheridan, License Plate Readers to be Used in D.C. Area, Wash. Post, Aug. 17, 2008, at C1.

[54] *See supra* note 66 and accompanying text.

[55] *See supra* note 87 and accompanying text.

B. WHETHER OR NOT USE OF ALPR TO CONDUCT MASS GOVERNMENTAL SURVEILLANCE SHOULD BE HELD UNCONSTITUTIONAL BY THE SUPREME COURT

It is imperative that the Supreme Court finally determine the constitutionality of conducting indiscriminate mass government surveillance of vehicular travels. *United States v. Jones*, a companion case of *Maynard*,[56] supra, is the most recent Supreme Court case with potential to provide guidance on this issue and modern phenomenon.[57] In *Jones*, the FBI procured a search warrant authorizing the installation of a tracking device on the defendant's vehicle.[58] 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 the warrant invalid.[59] Nonetheless, over the next 28 days, the device produced over 2,000 pages of data tracking the vehicle's movements, which connected defendant to an alleged co-conspirators' stash house that contained $850,000 in currency and 97 kilograms of cocaine.[60] Jones motioned to suppress all evidence obtained by tracking device in violation of the Fourth Amendment.[61] As mentioned in the *Maynard* discussion, *supra*,[62] the District of Columbia Court of Appeals ruled in favor of Jones and Maynard, co-conspirators, finding that the nearly month long tracking of the vehicle was unconstitutional absent a valid search warrant because it violated an expectation of privacy under the *Katz* test.[63]

The Supreme Court of the United States granted certiorari to review the Fourth Amendment issue.[64] 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* constitutional expectation of privacy test, *supra*.[65] Justice Scalia, writing for the Court, hinged the majority opinion on the fact that, by installing the GPS tracking device on the undercarriage of defendant's vehicle, the government trespassed on defendant's property.[66] According to Justice Scalia, this conduct amounted to "physically occup[ying] private property for the purpose of obtaining information."[67] Consequently,

---

[56] *Maynard*, 615 F.3d 544. *See supra* notes 66-72 and accompanying text.
[57] United States v. Jones, 132 S.Ct. 945 (2012).
[58] *Id*.
[59] *Id*.
[60] *Id*. at 948-49.
[61] *Id*.
[62] *See supra* notes 66-72 and accompanying text.
[63] *Maynard*, 615 F.3d at 564.
[64] *Jones*, 132 S.Ct. 945.
[65] *Id*. at 949. *See also supra* notes 25-28 and accompanying text.
[66] *Id*.
[67] *Id*.

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.'"[68] By deciding the case using trespass jurisprudence, which was applicable before the *Katz* test, Justice Scalia did not overturn *Katz* precedent, 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."[69]

In essence, instead of holding that the prolonged tracking of a vehicle's travels is unconstitutional because it violates a reasonable expectation of privacy under *Katz*, Justice Scalia merely made it unlawful for the government to install a tracking device on one's property without a valid warrant.[70] This 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 automobile travels using a more sophisticated means of surveillance (*i.e.*, ALPR cameras)? Under Justice Scalia's opinion, this tech-savvy method of automobile surveillance would ostensibly be permissible under the majority *Jones* opinion because it does not require a physical trespass on the vehicle. This loophole renders Justice Scalia's holding shortsighted and vulnerable to modern surveillance methods, such as ALPR. 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 be the dispositive consideration?

In *Katz v. United States*, the United States Supreme 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." 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 public telephone booth. Because the booth did not belong to the defendant, there could not be a showing of physical trespass.[71] However, the Court recognized that recording a person's telephone conversation in a closed phone booth, even if public property, violated an expectation of privacy that most individuals expect existed in the phone booth. Accordingly, this expectation of privacy is what the Court believed ought to be protected by the Fourth Amendment, not the existence or

[68] *Id.*
[69] *Id.* at 952.
[70] *Id.*
[71] *See id.*

absence of a physical trespass.[72] This principle is precisely what led to the modern two prong subjective and objective expectation of privacy test.[73]

Justice Scalia's reliance on the trespassory test to decide the surveillance issue in *Jones* only backtracks precedent on a constitutional issue of growing concern with the advent of technologically advanced means of surveillance. Acknowledging these concerns, Justice Alito criticized Justice Scalia's opinion as being "unwise" and "highly artificial" for applying "18th century tort law" to a "21st-century surveillance technique."[74] 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).[75]

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 expectation of privacy was violated by the four-week surveillance of his vehicle's movements.[76] Accordingly,

> [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.[77]

Justice Sotomayor, in a separate concurring opinion, illuminated why long term government surveillance of vehicular travels violates a reasonable expectation of privacy.[78] Like several other courts,[79] Justice

---

[72] *See id*.
[73] *Id*.
[74] *Jones,* 132 S.Ct. at 957-58 (Alito, J., concurring with Ginsburg, Breyer, and Kagan, J.J., joining).
[75] *Id*. at 961.
[76] *Id*. at 958.
[77] *Id*. at 964.
[78] Id. at 954-57.
[79] *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).

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."[80] For instance:

> [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.81

This information is even more intrusive when "[t]he Government can store such records and efficiently mine them for information years into the future."[82] Hence, Justice Sotomayor opined that long term tracking of a person's vehicular travels breaches an expectation of privacy the Fourth Amendment is intended to protect.[83]

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."[84] Second, because "the Fourth Amendment protects people, not places,"[85] the appropriate test should be to "ask whether people reasonably 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."[86] Justices Alito and Sotomayor have already answered in the negative.[87]

Understanding how the nine Justices voted in *Jones* provides insight on how each would vote with respect to whether using ALPR technology to track a vehicle's location is lawful. Chief Justice Roberts, as well as Justices Kennedy, Thomas and Sotomayor joined Justice Scalia's opinion, making it the majority.[88] However, had Justice Sotomayor joined Alito's concurrence instead, then Justice Alito's opinion would constitute

[80] *Jones,* 132 S.Ct. at 956.
[81] *Id*.
[82] *Jones,* 132 S.Ct. at 955-56.
[83] *Id*. at 955.
[84] *Id*.
[85] *Katz*, 389 U.S. at 351.
[86] *Jones*, 132 S.Ct. at 955.
[87] *Id*. at 955, 964.
[88] *Id*. at 947.

the majority because Justices Ginsburg, Breyer, and Kagan all joined.[89] Nonetheless, the concurrences of Justice Alito and Sotomayor command five votes. Consequently, a potential majority of the current members of the Supreme Court, not only advocate application of the *Katz* test on this issue, but believe that long term monitoring of one's travels impinges on a reasonable expectation of privacy, thereby constituting a search within the meaning of the Fourth Amendment.

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, it would be imprudent to wait until the constitutional issue reaches the Court again. The Constitution sets the minimal protections against State action, 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 accomplishing this goal 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."[90]

However, for the legislation to be effective, it is essential that it balance two distinct competing interests. The legislation must be carefully drafted to: (1) permit law enforcement agencies to employ ALPR devices for its valuable crime solving capabilities; as well as: (2) draw effective boundaries to ensure it is not used as a tool for conducting indiscriminate and ubiquitous government surveillance without a valid search warrant.

The Electronic Communications Privacy Act is a federal law that currently governs the use of wiretapping and electronic eavesdropping.[91] 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 acquire geolocation information."[92]

In the interest of justice, however, the ECPAA provides for an exigency exception to the search warrant requirement if there are grounds to believe that a search warrant could be obtained, but the acquisition of a

[89] *Id*. at 957.
[90] *Id*. at 964.
[91] *Id*.
[92] S. 1011, 112th Cong., 1st Sess. (2011). Senator Ron Wyden and Representative Jason Chaffetz have introduced nearly identical legislation, entitled the Geolocational Privacy and Surveillance Act, or GPS bill. S. 1212, H.R. 2168, 112th Cong., 1st Sess. (2011).

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.[93] Nonetheless, this warrant exception is limited because, "not later than 48 hours after the activity to acquire the geolocation information has occurred," the government must seek a warrant.[94] 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.[95] 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 subject's consent.[96]

The ECPAA makes the unwarranted use of ALPR's geolocation memory feature unlawful by proscribing the devices current method of operation, which is a robotic collection and retention of the geolocation information of every vehicle the device captures on camera, regardless of due consideration to reasonable suspicion of criminal activity. Hence, this bill would effectively ban ALPR's use as a tool to conduct indiscriminate mass surveillance of vehicular movements. Nonetheless, the bill's exigency exception effectively balances law enforcement and public safety needs by permitting the device to be used without a warrant in an enumerated category of 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. Hence, the ECPAA bill successfully provides the proper balance needed to level the privacy and public policy concerns associated with use of ALPR technology.

CONCLUSION

The United States Supreme Court, as well as district, circuit, and state courts around the country, have all acknowledged the potentially devastating effects mass surveillance of vehicular travels can have on Fourth Amendment rights. Unaware that this threat can be implemented today, the judiciary has been presented with the opportunity, but refused,

[93] S. 1011, 112th Cong., 1st Sess, 18 USC § 2713(d)(1).
[94] S. 1011, 112th Cong., 1st Sess, 18 USC § 2713(d)(2)(a).
[95] S. 1011, 112th Cong., 1st Sess, 18 USC § 2713(d)(2)(b).
[96] S. 1011, 112th Cong., 1st Sess, 18 USC § 2713(d)(3)(a).

on several occasions to rule directly on the constitutionality of this issue. However, with the growing ubiquity of ALPR cameras, mass government surveillance of automobile travels is a phenomenon that, if not regulated, can be implemented today. As such, 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 technology such as this could gradually lead to a world of Orwellian-like surveillance and reshape modern-day expectations of privacy.