1-1-2016

Ohio is Jonesing for Automatic License Plate Readers: Why This May Violate Your Fourth Amendment Rights and What The Ohio Legislature Should Do About It

Michael E. Fisher
Cleveland-Marshall College of Law

OHIO IS JONESING FOR AUTOMATIC LICENSE PLATE READERS: WHY THIS MAY VIOLATE YOUR FOURTH AMENDMENT RIGHTS AND WHAT THE OHIO LEGISLATURE SHOULD DO ABOUT IT

MICHAEL E. FISHER*

ABSTRACT

The City of Cleveland currently owns and operates several automatic license plate recognition cameras. With a quick scan these cameras can provide law enforcement with locational and other personal data about an individual. The Supreme Court in *United States v. Jones* successfully avoided the issue of whether there is a privacy right in locational data; thus this Note addresses the need for Ohio legislation in order to balance the interests of law enforcement in using license plate data to apprehend criminals with citizens' Fourth Amendment right to be free from unreasonable searches and seizures. The Note examines legislation in effect in other states regarding automatic license plate recognition systems and uses this legislation to propose recommendations for the Ohio Legislature.

CONTENTS

* J.D. expected, Cleveland-Marshall College of Law, May 2016. Special thanks due to Professor Alex Frondorf for his advice and guidance throughout the research and writing process. I would like to extend my appreciation to my advisor, Professor Stephen Lazarus, for his willingness to oversee the writing of this paper. Deepest thanks to Jeffrey Fisher and Virginia Fisher for their encouragement and inspiration. I would also like to thank Emily Louise Wallace for her never-ending support.

I. THE ISSUE PRESENTED BY CLEVELAND'S RECENT ACQUISITION OF LICENSE PLATE READERS

In 2012, the City of Cleveland purchased sixteen high-speed cameras to be used in automatic plate recognition systems.[1] When mounted to a police vehicle that is driving at a high rate of speed, a single camera is capable of scanning 1,800 license plates per minute, recognizing license plates from all fifty states, and recording locational data for each plate scanned.[2] This information is then stored in large databases and each individual license plate scan is checked to see if it matches the license plate of any stolen vehicle or any vehicle used in the commission of a crime.[3] If there is a match, the officer driving the police vehicle is notified instantly.[4] In a perfect world, this instant feedback allows the officer to stop the car, identify the person driving the car as the person suspected of the crime in the database, and then apprehend the individual.[5]

This instant identification creates a significant increase in the efficiency of police work. However, the efficiency comes at the expense of citizens' constitutionally protected right to be free from unreasonable searches and seizures. Such a violation of the Fourth Amendment is unconstitutional, but for citizens in states without policies regarding the use of automatic license plate recognition systems, it may be the norm. The reason behind this result is that the use of automatic license plate recognition systems results in the collection of a massive amount of license plate scans that contain data concerning the daily travels of innocent, suspicionless citizens.[6] Though the harm of a single scan may be miniscule, combining years' worth of scans of a single license plate may paint a vivid picture of an innocent

---

[1] American Civil Liberties Union, Receipt for Public Records Request, City of Cleveland Dep't of Law (Sept. 21, 2013), https://www.aclu.org/files/FilesPDFs/ALPR/ohio/14632-14733%20Cleveland.pdf.

[2] *Mobile Plate Hunter-900*, ELSAG NORTH AMERICA, http://elsag.com/mobile.htm (last visited Jan. 13, 2016).

[3] AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 5 (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

[4] *Id.*

[5] *Id.*

[6] For the purpose of this Note and for reasons of brevity, I am not able to conduct an empirical study of all license plate scans in the United States.

person's daily patterns and behaviors.[7] Statistics reported by states that have adopted automatic license plate recognition systems demonstrate that fears of such Fourth Amendment intrusion are not off base. For example, in 2012, for every one-million license plates scanned in Maryland only forty-seven scans were potentially associated with "serious crimes."[8] Despite the fact that many states hover around Maryland's dismal .0047% hit rate, many police departments still collect and store the data associated with these non-hit scans.[9] The length of time such data is stored varies. Some states keep the data indefinitely,[10] and some policies require deletion of non-hit data after five years.[11] Such storage practices provide a great deal of locational data on innocent people that can be mined to determine their daily patterns and behaviors.

This is a difficult problem to fix judicially because automatic license plate recognition technology is rapidly expanding, and therefore it presents virtually unprecedented challenges to the courts. A recent United States Supreme Court case displays the judicial system's reluctance to decide whether individuals have a reasonable expectation of privacy in their locational data collected by technology similar to automatic license plate recognition systems. The novelty of the issues presented by modern technology combined with the Court's judicial restraint results in unworkable tests, which demonstrates the need for legislative intervention. Unfortunately, many states and police departments have not adopted legislation or policies regarding the use of automatic license plate recognition systems, but instead employ this technology as soon as funding is available, leaving citizens unprotected against the intrusion of government into their private lives.

This Note first explores the history and evolution of the Fourth Amendment, starting with the concerns of the Framers and then the transition from a property-based inquiry to a reasonable expectation of privacy test for determining Fourth Amendment issues. Then this Note explains the Supreme Court's decision in *United States v. Jones* and the its avoidance of the modern day issue as to whether there is a right to privacy in locational data. This Note then analyzes the concurring opinions in *Jones*, which explicitly call for legislation regarding this issue. Finally, this Note reviews automatic license plate recognition legislation in effect in other states and proposes recommendations for the Ohio Legislature.

---

[7] This is called the "mosaic theory." For an overview of the mosaic theory, see Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733 (2011).

[8] AM. CIVIL LIBERTIES UNION, *supra* note 3, at 14. "Serious crimes" include stolen vehicles, wanted persons, violent gangs, terrorist organizations, or sex offenders." *Id.*

[9] *See id.* at 15. Rhinebeck, New York, in a three-month period scanned 99,771 license plates resulting in a .01% hit rate. *Id.* High Point, North Carolina, in an eleven-month period scanned 70,289 license plates resulting in a .08% hit rate. *Id.* Burbank, Illinois in a one-year period scanned 706,918 license plates resulting in a 0.3% hit rate. *Id.*

[10] *Id.* at 20.

[11] N.J. Att'y Gen., Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (Dec. 3, 2010), http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf.

II. THE EVOLVING FOURTH AMENDMENT AND THE EXPECTATION OF PRIVACY

The Fourth Amendment to the United States Constitution, adopted in March 1792, reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[12]

The original intent of the Framers was to put an end to writs of assistance and general warrants that were used to forcibly enter colonists' homes with little basis so the British could ransack their homes in search of libelous books.[13] This is a far cry from concerns raised by privacy advocates today, such as the public outcry that led to the demise of the creation of a national automatic license plate recognition ("ALPR") system in early 2014.[14]

From the adoption of the Fourth Amendment until 1967, the Supreme Court treated Fourth Amendment issues as property-based inquiries that required trespass of a person's personal property to trigger a Fourth Amendment violation.[15] The Court departed from the trespass standard in 1967 in its landmark decision in *Katz v. United* States.[16] In *Katz*, the defendant Charles Katz was charged with violating a federal law prohibiting the use of interstate communications for placing wagers and bets.[17] Law enforcement agents witnessed Katz make numerous calls from a telephone booth, and afterwards the agents placed microphones on the outside of the booth to eavesdrop on Katz's conversation.[18] Using this information Katz was convicted in the district court, and the Ninth Circuit Court of Appeals affirmed.[19] The Supreme Court rejected the parties' discussion of whether the telephone booth was a constitutionally protected area under the property-based trespass theory.[20] Instead, the Court adopted the reasonable expectation of privacy test and held that the defendant assumed his conversations were private because he sought to exclude

---

[12] U.S. CONST. amend. IV.

[13] William C. Koch, *The Warrant Requirement*, *in* 1 ENCYCLOPEDIA OF THE FOURTH AMENDMENT 18-22 (John R. Vile & David L. Hudson, Jr., eds., 4th ed. 2013); *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990).

[14] *See* Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-Plate Tracking Plan*, WASH. POST (Feb. 19, 2014), https://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-0204122c514b_story.html.

[15] John R. Vile, *Trespass Actions*, *in* 2 ENCYCLOPEDIA OF THE FOURTH AMENDMENT 627-28 (John R. Vile & Daniel L. Hudson, eds., 4th ed. 2013).

[16] 389 U.S. 347 (1967).

[17] *Id.* at 348.

[18] *Id.*

[19] *Id.*

[20] *Id.* at 351-53.

others when he entered the enclosed telephone booth.[21] The Supreme Court concluded, "[t]he government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[22]

In 1983, the Supreme Court cited *Katz* when determining whether a defendant had a reasonable expectation of privacy when traveling on a public road.[23] In *United States v. Knotts*, the government placed a radio transmitter in a container of chloroform to track the movements of the vehicle holding the container.[24] The radio transmitter data led the government to a remote cabin where a warranted search revealed a drug lab.[25] The Court determined that no search occurred during the tracking of the vehicle because, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[26]

A year later, in *United States v. Karo*, the Court heard a case in which police placed a radio transmitter in a can of ether that allowed them to track the location of the defendant.[27] The radio transmitter data led the government to a private residence where they executed a search warrant that led to the discovery of cocaine and drug manufacturing equipment.[28] In accord with *Katz* and *Knotts*, the Court held that the locational data received while the radio transmitter was on public roads was constitutional because Karo did not have a reasonable expectation of privacy while driving on the roads.[29] However, the Court held that monitoring the device while in

---

[21] *Id.* at 353.

[22] *Id.*

[23] United States v. Knotts, 460 U.S. 276, 280 (1983) (citing Katz v. United States, 389 U.S. 347 (1967)). In citing *Katz*, the Court relied heavily on a quote from *Smith v. Maryland*, 442 U.S. 735 (1979), in which the Court elaborated on the principles in *Katz*. *See Knotts*, 460 U.S. at 480-81 ("Consistently with *Katz,* this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry, as Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy' . . . . The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable' . . . .") (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[24] *Knotts*, 460 U.S. at 277.

[25] *Id.* at 279.

[26] *Id.* at 281. The Court further observed, "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways. We have commented more than once on the diminished expectation of privacy in an automobile . . . ." *Id.*

[27] United States v. Karo, 468 U.S. 705, 708 (1984).

[28] *Id.* at 710.

[29] *Id.* at 721.

the private residence was unconstitutional under the Fourth Amendment.[30] The Court distinguished *Knotts* in reaching the latter part of that holding because, in *Knotts*, the beeper was not monitored while inside a private residence;[31] whereas in *Karo* the beeper was monitored inside a private residence.[32] This was evidenced by the affidavit supporting the application for a search warrant explicitly stating that, "[u]sing the 'beeper' locator, I positively determined that the 'beeper' can . . . was now inside the above-described premises."[33] Until 2012, the Supreme Court was fairly consistent in its analysis of Fourth Amendment issues presented by cases with facts similar to the ones just described.

A. United States v. Jones*: The Application of* Knotts *and the Continuing Evolution*

In a 2012 Supreme Court case, *United States v. Jones*, the Court decided a modern Fourth Amendment issue similar to those in *Katz* and *Knotts*.[34] In *Jones*, the defendant Antoine Jones was suspected of trafficking narcotics and was made the target of an investigation by a joint FBI and D.C. Metropolitan Police Department task force.[35] Based on data gathered through the use of cameras outside the nightclub owned by Jones, visual surveillance, and wiretaps of his personal cellphone, the government applied for and was granted a warrant.[36] The warrant authorized government agents to install a GPS device on Jones's vehicle in the District of Columbia within ten days.[37] However, agents did not install the GPS device until the eleventh day, in a parking lot in Maryland.[38] Over the next twenty-eight days the GPS device yielded more than two-thousand pages of data.[39] The data allowed the government to track Jones and ultimately obtain a multiple-count indictment charging Jones and several alleged co-conspirators with conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and fifty grams or more of cocaine base.[40]

---

[30] *Id.* at 714-15. "[In *Knotts*] [t]he Court held that since the movements of the automobile and the arrival of the can containing the beeper in the area of the cabin could have been observed by the naked eye, no Fourth Amendment violation was committed by monitoring the beeper during the trip to the cabin. In *Knotts*, the record did not show that the beeper was monitored while the can containing it was inside the cabin, and we therefore had no occasion to consider whether a constitutional violation would have occurred had the fact been otherwise." *Id.* at 713-14.

[31] *Id.* at 714. "In *Knotts*, the record did not show that the beeper was monitored while the can containing it was inside the cabin, and we therefore had no occasion to consider whether a constitutional violation would have occurred had the fact been otherwise." *Id.*

[32] *Id.* at 714.

[33] *Id.*

[34] *See* United States v. Jones, 132 S. Ct. 945 (2012).

[35] *Id.* at 948.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

Before trial, Jones filed a motion to suppress evidence obtained through the GPS device.[41] The district court granted the motion as it pertained to the data obtained while the vehicle was parked on Jones's property, but the district court held that the data obtained through the GPS device while the vehicle was on public roads was admissible.[42] In reaching this decision the district court relied on Supreme Court precedent in *Knotts* stating that, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[43] Jones's October trial resulted in a hung jury on the conspiracy count, but in March 2007 a grand jury charged Jones with the same conspiracy.[44] Using the same GPS data admitted in the first trial the jury returned a guilty verdict, and the district court sentenced Jones to life in prison.[45]

Jones appealed the decision. The United States Court of Appeals for the District of Columbia reversed Jones's conviction,[46] holding that the evidence obtained by the warrantless use of the GPS device violated the Fourth Amendment, and therefore the admission of such evidence was improper.[47] The D.C. Circuit denied the government's petition for rehearing en banc, with four judges dissenting, after which the Supreme Court granted certiorari.[48]

III. ANALYSIS

A. Jones *Majority: Avoiding the Issue of Individuals' Right to Privacy in Locational Data*

Legal scholars,[49] privacy advocates,[50] and even average citizens[51] anticipated the Supreme Court's review of the lower court's decision in *Jones* because it appeared

---

[41] *Id.*

[42] *Id.*

[43] United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (quoting United States v. Knotts, 460 U.S. 276, 281-82 (1983), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)).

[44] *Jones*, 132 S. Ct. at 948.

[45] *Id.* at 949.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *See* Jace C. Gatewood, *It's Raining* Katz *and* Jones*: The Implications of* United States v. Jones*—A Case of Sound and Fury*, 33 PACE L. REV. 683, 683-84 (2013). "The *Jones* case garnered widespread coverage across the nation, and became a polarizing topic of discussion especially among lawyers, judges, legal commentators, and law students. Even the average person on the street seemed to have an opinion regarding the authority of the government to secretly track the public movements of a person in everyday life." *Id.*

[50] Jessica Monaco, *This Week in Civil Liberties*, AM. CIV. LIBERTIES UNION BLOG (July 1, 2011), https://www.aclu.org/blog/week-civil-liberties.

[51] *See, e.g.*, Robert Barnes, *Supreme Court Worries That New Technology Creates '1984' Scenarios*, WASH. POST (Nov. 8, 2011), https://www.washingtonpost.com/politics/supreme-court-worries-that-new-technology-creates-1984 scenarios/2011/11/08/gIQAbHdw2M_story.html.

that the Supreme Court would finally reach a decision "regarding the authority of the government to secretly track the public movements of a person in everyday life."[52] However, this issue was not ultimately resolved in *Jones*. In fact, the Supreme Court nearly avoided the issue altogether by reverting to its property-based inquiry decisions from 1928 and 1942. [53]

In *Jones,* the government did not execute the warrant within the ten-day time frame (installing the device on the eleventh day) and did not adhere to the requirement that the GPS device be placed on the car in D.C. (device was placed on the car in Maryland); therefore, at the time the government placed the device on the car it did not have a valid warrant.[54] Justice Scalia, in writing for the five-member majority, expressed no doubt that a vehicle was an "effect" under the language of the Fourth Amendment[55] or that the placing of the device on the car was considered a "search."[56]

The government cited *Katz* in its argument that that no search occurred since Jones had no "reasonable expectation of privacy" in the area of the vehicle accessed by government agents and in the locations of the vehicle on the public roads since they were visible to the public.[57] Nevertheless, Justice Scalia thought it was more significant that the government had trespassed on Jones's property when installing the device.[58] In so holding, the five-member majority avoided deciding the much larger issue of whether Jones's reasonable expectation of privacy was violated by the long-term use of the GPS tracking device to monitor the movements of his vehicle.

Under the majority reasoning in *Jones*, if it were technologically possible to track a person using a GPS-type device without physically trespassing on that person's property, the government would not need a warrant to monitor that person's daily whereabouts. This issue is important because this technology exists in many forms, especially in automatic license plate recognition systems. The automatic license plate recognition systems make it possible for the government to monitor people in ways that are as invasive as the aforementioned cases while still managing to avoid a physical trespass. Thus, automatic license plate recognition technology enables the government to perform an end run around the property-based inquiry reverted to by Justice Scalia. For this reason, it is easy to see why this decision disappointed those

---

[52] Gatewood, *supra* note 49, at 683-84.

[53] *See Jones,* 132 S. Ct. at 953-54; *see also id.* at 959 (Alito, J., concurring) (citing Goldman v. United States, 316 U.S. 129, 138 (1942); Olmstead v. United States, 277 U.S. 438, 471 (1928)).

[54] *Id.* at 948 n.1 (majority opinion).

[55] U.S. CONST. amend. IV ("The right of the people to be secure in their . . . effects, against unreasonable searches . . . .").

[56] *Jones*, 132 S. Ct. at 949.

[57] *Id.* at 950.

[58] *Id.* at 949. ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

who anticipated the lasting impact on Fourth Amendment jurisprudence that *Jones* could have had.[59]

B. Jones *Concurrence*

In keeping with Justice Scalia and Justice Thomas's originalist approach to constitutional interpretation, the majority opinion departed from the reasonable expectations test set out in *Katz* in favor of eighteenth-century tort law principles supporting an action for trespass to chattels.[60] While four of the Justices concurred with the Court's holding to exclude the evidence, they disagreed with the majority's approach to such a modern technology case.[61] One of the main reasons the concurring Justices disagreed with this departure from the *Katz* test was because the majority opinion and use of precedent did not deal with cases in which the government relied on electronic tracking that did not involve a trespass.[62]

The concurring Justices' logic in *Jones* is not unprecedented in Fourth Amendment cases. *Goldman v. United States* and *Olmstead v. United States* from 1942 and 1928 produced dissenting opinions attempting to address the issue of technological advancements under the Fourth Amendment.[63] In *Goldman*, Justice Murphy, in a dissenting opinion, argued that new technology made invasions of privacy possible that did not require a physical trespass but they were still every bit as offensive to the Fourth Amendment as a trespass.[64] Justice Brandeis, in *Olmstead*, argued that the Fourth Amendment language should be broadly interpreted and applicable to modern issues.[65] The concurring Justices' reasoning in *Jones* was no different.

---

[59] Gatewood, *supra* note 49, at 683 ("Reading the highly anticipated decision of *United States v. Jones* . . . was much like waking up Christmas morning only to find out that you did not get everything on your Christmas list. Santa not only did not bring you everything on your list, but also forgot all the good stuff. So, all of the excitement and anticipation of the moment yields way to 'Bah! Humbug!' feelings, and the long awaited moment becomes merely a footnote in annals of Christmases past.").

[60] *Jones*, 132 S. Ct. at 953. "At common law, a suit for trespass to chattels required merely a violation of 'the dignitary interest in the inviolability of chattels,' but today there must be 'some actual damage to the chattel before the action can be maintained.'" *Id.* at 957 n.2 (Alito, J., concurring) (quoting W. KEETON, D. DOBBS, R. KEETON, & D. OWEN, PROSSER & KEETON ON LAW OF TORTS 87 (5th ed. 1984)). In *Jones*, no damage was done to Jones's vehicle when the tracking device was attached. *Id.*

[61] *See id.* 957-58 (Alito, J., concurring).

[62] *Id.* at 961-62.

[63] *See* Goldman v. United States, 316 U.S. 129, 138 (1942) (Murphy, J., dissenting); Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

[64] *Goldman,* 316 U.S. at 139. ("[S]cience has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment. Surely the spirit motivating the framers of that Amendment would abhor these new devices no less. Physical entry may be wholly immaterial.").

[65] *Olmstead*, 277 U.S. at 473-74. ("Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, 'in the application of a

In concurring, Justice Alito wrote, "[r]ecent years have seen the emergence of many new devices that permit the monitoring of a person's movements," and "[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."[66] He then went on to say that, in the absence of congressional legislation on this matter, courts are bound to decide these issues under the current Fourth Amendment doctrine and "ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[67] Under this approach, the use of longer term GPS monitoring in investigations of most offenses would intrude on a reasonable person's expectation of privacy.[68]

Justice Sotomayor filed a separate concurrence in which she disagreed with Justice Alito that the physical intrusion element is completely irrelevant;[69] however, she did recognize that physical intrusion is now unnecessary to many forms of surveillance and that long-term GPS monitoring in investigations of most offenses intrudes on expectations of privacy.[70] Prior to the Court's decision in *Jones*, many cities, including Cleveland, already had adopted surveillance technologies of the kind that Justice Sotomayor warned the Court about.[71]

IV. A CALL FOR LEGISLATION

Constitutional interpretation in light of rapidly advancing technology produces unworkable tests and avoids answering critical privacy issues.[72] This dilemma was noted in both concurring opinions in *Jones*. Justice Alito wrote, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may

---

Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping.") (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[66] *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring).

[67] *Id.* at 964.

[68] *Id.*

[69] *See id.* at 955 (Sotomayor, J., concurring) ("Justice Alito's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. By contrast, the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.").

[70] *Id.* ("[A]s Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones . . . . In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. 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.") (internal citations omitted).

[71] *See supra* Part I.

[72] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004).

be legislative."[73] He then, almost reluctantly, explains that in light of the fact that Congress has not enacted any legislation regulating the use of GPS-tracking technology for law enforcement purposes, "[t]he best that we can do . . . is to apply existing Fourth Amendment doctrine . . . ."[74] Justice Sotomayor also seemed hesitant in light of the fact that there is no congressional oversight into this matter. In her concurring opinion she states, "I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse . . . ."[75] At the end of the majority opinion, Justice Scalia notes that surveillance, which does not intrude on a citizen's property, could potentially be unconstitutional but that the facts in *Jones* did not require the Court to resolve this issue yet.[76] One can only imagine that Justice Scalia, exercising his judicial restraint, felt these problems were better left to the legislature if they are to be resolved anytime soon. Likewise, both concurring opinions are a call for legislation regarding these matters.

The importance of this issue is apparent when looking at two bills introduced in Congress. Despite the fact that the bills do not directly address the issue of automatic license plate recognition systems, the issue of locational privacy is on the minds of some legislators. On June 15 and 16, 2011, just five months before oral arguments in *Jones* and seven months before the *Jones* decision, two bills seeking to regulate GPS surveillance were introduced in Congress. The Geolocational Privacy and Surveillance Act sought to amend title 18 of the United States Code to specify the circumstances in which a person may acquire geolocation information.[77] Under this Act, "geolocation information" is defined as:

> [A]ny information . . . concerning the location of a wireless communication device or tracking device . . . that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.[78]

---

[73] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (citing Kerr, *supra* note 72, at 805-06).

[74] *Id.* For two separate interpretations of Justice Alito's "[t]he best we can do" language, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 351 n.233 (2012). On the one hand, Professor Kerr says that this language reflects the constitutional avoidance doctrine and on the other hand that the language evinces a combination of judicial application of the mosaic theory by the judiciary along with congressional oversight. Because *Jones* involved federal agents that likely would not have been bound by state statute Kerr seems to think this interpretation is stronger, *see id.* at 351-52, but for the purpose of introducing other state legislation and advocating a call to the Ohio General Assembly in light of *State v. Johnson*, 22 N.E.3d 1061 (Ohio 2014), I have only discussed the former constitutional avoidance interpretation.

[75] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

[76] *Id.* at 954 (majority opinion) ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

[77] Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011).

[78] *Id.* § 2.

This would appear to cover the device that was physically attached to the vehicle in *Jones* but would not prohibit the type of tracking accomplished by automatic license plate recognition systems. Moreover, the Location Privacy Protection Act of 2012 sought to address voluntary location tracking of electronic communications devices.[79] Similar to the other Bill, the Location Privacy Act of 2012 does not directly address automatic license plate recognition systems but defines the prohibited device as one that is "designed or intended to be carried by or on the person of an individual or travel with the individual, including, but not limited to, a vehicle the individual drives."[80] This language appears to address physically attached devices such as the one used in *Jones,* but would not appear to address automatic license plate recognition systems since those are not carried or attached to a vehicle. Nevertheless, these Bills provide insight into the minds of some legislators despite the fact that neither Bill was passed in this form.[81]

The Locational Privacy Act of 2012 was resubmitted on March 17, 2014, and is still under consideration.[82] In its current form the Bill differs from the original in that it defines the prohibited device as one "commonly carried by or on the person . . . or commonly travels with the individual, including in or as part of a vehicle the individual drives."[83] This does not appear to limit the device to one that is designed or intended to be carried, or to one that is attached to a person or vehicle, as in the previous version, and actually expands the number of devices that are covered.[84] The fact that this Bill was amended two years later to expand the type devices covered represents the rapidly evolving technology that must be regulated.[85] Even if this Bill were to pass it does not appear to regulate technologies, such as the automatic license plate recognition systems, that many cities, including Cleveland, have already adopted.[86]

V. WHY THIS ISSUE MATTERS TO OHIO CITIZENS

This issue matters to Ohio citizens because automatic license plate recognition technology has been implemented in Ohio cities and Ohio courts have recently faced Fourth Amendment issues caused by locational data privacy. In March 2014, the Ohio Supreme Court was faced with substantially similar facts and issues presented in *Jones*.[87] The case was an appeal from a 2010 conviction decided prior to the

---

[79] *See* Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

[80] *Id.* § 3.

[81] *See Location Privacy Protection Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/s2171 (last visited Dec. 6, 2015) [hereinafter GOVTRACK S. 2171]; *Geolocations Privacy and Surveillance Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/s1212/text (last visited Dec. 6, 2015).

[82] GOVTRACK S. 2171*, supra* note 81.

[83] Location Privacy Protection Act of 2014, S. 2171, 113th Cong. § 3 (2014) (reintroduced from a previous session of Congress).

[84] *See id.*

[85] *See* discussion *supra* Part I.

[86] *See* discussion *supra* Part I.

[87] *See* State v. Johnson, 22 N.E.3d 1061 (Ohio 2014).

ruling in *Jones*.[88] In this case, a County Sheriff's Deputy from Butler, Ohio, acting without a warrant, attached a GPS tracking device to the defendant's vehicle while it was parked on the street across from his home in October 2008.[89] The deputies tracked the defendant's van for five days, culminating in a traffic stop conducted at gunpoint.[90] No drugs were found in the defendant's vehicle, but drugs were found in his associate's vehicle, which had also been stopped.[91] At trial the defendant's motion to suppress the GPS evidence was denied and he was sentenced to fifteen years in prison.[92] The Twelfth District Court of Appeals affirmed the denial of his motion to suppress holding that the placement of the GPS device on his vehicle was not a search for purposes of the Fourth Amendment.[93] In March 2012, the Ohio Supreme Court accepted the defendant's appeal and vacated the District Court of Appeals' judgment and remanded to the trial court for the application of *Jones*.[94] On remand, the trial court found that placing the GPS tracking device on the defendant's van violated the Fourth Amendment but declined to suppress the evidence based on the "good-faith" exception to exclusionary rule.[95] The defendant was sentenced to ten years in prison.[96] The Twelfth District affirmed the trial court's decision, and in November 2014 the Ohio Supreme Court granted review.[97] The Ohio Supreme Court affirmed the conviction on the reasoning that the deputies acted with a good faith and objectively reasonable belief that the search would not violate defendant's Fourth Amendment rights based on the state of the law in October 2008.[98]

---

[88] *Id.* at 1064.

[89] *Id.* at 1063.

[90] *Id.*

[91] *Id.*

[92] *Id.* at 1063-64.

[93] *Id.* at 1064.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.* at 1065.

[98] *Id.* at 1070. ("In the aftermath of *Jones*, police officers can no longer harbor a good-faith belief that attaching a GPS tracking device to a vehicle is not a search for purposes of the Fourth Amendment. Nonetheless, at the time Detective Hackney attached the GPS device to Johnson's van, he acted with an objectively reasonable good-faith belief that his actions comported with the Fourth Amendment."). In acting on this state of the law belief in October 2008 the court relied on two cases cited above and stated, "when Detective Hackney attached a GPS tracking device to Johnson's van, two cases from the United States Supreme Court—*United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Karo*, 468 U.S. 705 (1984)—supported Hackney's objectively reasonable belief that attaching a tracking device to a vehicle did not violate any reasonable expectation of privacy that Johnson had, either in the undercarriage of his van or in his whereabouts while driving on public streets and highways." *Id.* at 1062.

This Ohio case and the "state of the law in October 2008" reasoning is a microcosm of the much larger problem: absent legislative regulation of rapidly evolving surveillance technologies, law enforcement agencies that adopt them will be able to remain one step ahead of a judicial system that seems to be approaching such issues at a snail's pace. The *Jones* approach does not reach the issues facing our modern society, especially issues that Ohio faces in light of Cleveland's purchase of sixteen new automatic license plate recognition systems.[99] Therefore, much like the Supreme Court's decision in *Jones*, this recent Ohio decision also avoids reaching crucial issues and further clarifies the need for legislative intervention.

A. It is Not Just Ohio

Responses to a document request under the Freedom of Information Act by the American Civil Liberties Union revealed the existence of a national license plate scanning database being built by the Department of Justice.[100] The initial scope of the project was aimed at combatting drug trafficking by drug cartels near the border.[101] Suspiciously, this does not explain the use of automatic license plate recognition cameras in New Jersey;[102] however, a brief look at New Jersey's guidelines for automatic license plate reader cameras reveals policies in favor of automatic license plate recognition systems and may provide an explanation as to why the Department of Justice has deployed cameras in New Jersey.[103] Since then, it appears that other state law enforcement agencies are accessing the database for assistance with their own ongoing investigations. The prevalence of these automatic license plate recognition systems highlights the urgency for legislation in these areas. The following sections provide an overview of states that currently have legislation or procedures in place to deal with the automatic license plate recognition issues.

VI. SOLVING THE AUTOMATIC LICENSE PLATE SCANNING ISSUE AT THE STATE LEVEL

Eight states have responded to the locational privacy issues raised by automatic license plate recognition systems by enacting legislation or issuing administrative opinions regarding the use of such systems.[104] The legislation at the state level ranges from significantly restricting the use of automatic license plate recognition systems,[105] to greatly expanding their use.[106] Exploring the legislation from these

---

[99] *See* discussion *supra* Part I.

[100] American Civil Liberties Union, DEA National License Plate Recognition Program, https://www.aclu.org/files/assets/Pages%20from%2030890-30907%202013.08.28%20-%20DEA%20Response.pdf (last visited Dec. 6, 2015).

[101] *See id.*

[102] *Id.*

[103] *See* discussion *infra* Part IV.D. Out of the state legislation and guidelines reviewed in this Note, New Jersey's policies are the most in favor of the use of automatic license plate recognition systems.

[104] ARK. CODE ANN. § 12-12-1803 (West 2015); CAL. VEH. CODE § 2413 (West 2015); ME. REV. STAT. tit. 29-A, § 2117-A (2015); N.H. REV. STAT. ANN. § 261:75-b (2015); N.J. Att'y Gen., Directive No. 2010-5, *supra* note 11; UTAH CODE ANN. § 41-6a-2003 (West 2015); Va. Att'y Gen., Legality of Collection from Automated License Plate Reader, 2013 WL 653025, at *4 (Feb. 13, 2013); VT. STAT. ANN. tit. 23, § 1607 (West 2015);.

[105] *See, e.g.*, N.H. REV. STAT. ANN. § 261:75-b (2015).

states paves the way for Ohio to adopt similar legislation that strikes a balance between protecting citizens' Fourth Amendment rights while still allowing law enforcement agencies utilizing the automatic license plate recognition systems to apprehend criminals.

A. Maine, New Hampshire, and California Enact Strict Legislation for Automatic License Plate Recognition Systems

Maine and New Hampshire have enacted the most restrictive automatic license plate recognition system legislation out of the eight states that have addressed this issue.[107] The New Hampshire State Highway Law prohibits all use of automatic license plate recognition cameras as well as other devices capable of "determining the ownership of a motor vehicle or the identity of a motor vehicle's occupants on the public ways of the state."[108] There are a few narrow exceptions carved out that allow camera use if it is undertaken for purposes of operation of a toll collection system,[109] to assist in securing three named bridges in Portsmouth,[110] and when the surveillance is incidental to the monitoring of a building or other structure under the control of the state.[111] This law further prohibits the State of New Hampshire and its political subdivisions from obtaining any information from outside sources that it would not be able to obtain itself under the exceptions just mentioned.[112] This means that the law enforcement agencies in New Hampshire may only access other automatic license plate recognition databases if the scans fall into one of the narrow exceptions mentioned above.

Maine's legislation prohibits private use of automatic license plate recognition cameras and requires law enforcement to delete stored license plate data that is not part of a criminal investigation within twenty-one days.[113] This is three days shorter than New Hampshire's twenty-four day time limit for storing license plate data.[114] Similar to New Hampshire's statute, Maine's statute exempts the turnpike authority or a law enforcement agency using the cameras for toll enforcement purposes. [115]

---

[106] *See, e.g.,* N.J. Att'y Gen., Directive No. 2010-5, *supra* note 11.

[107] *See* N.H. REV. STAT. ANN. § 261:75-b (2015) (prohibiting, with limited exceptions, the use of automated number plate scanning devices); ME. REV. STAT. tit. 29-A, § 2117-A (2015) (also prohibiting, with limited exceptions, the use of automated number plate scanning devices).

[108] N.H. REV. STAT. ANN. § 236:130(I) (2015).

[109] *Id.* § 236:130(III)(e).

[110] *Id.* § 236:130(III)(f).

[111] *Id.* § 236:130(III)(g).

[112] *Id.* § 236:131 ("Neither the state of New Hampshire nor its political subdivisions shall obtain from others, including private businesses and federal and state governments, any information that it is prohibited from obtaining under the provisions of RSA 236:130.").

[113] ME. REV. STAT. tit. 29-A, § 2117-A(5) (2015).

[114] N.H. REV. STAT. ANN. § 236:130(III)(g) (2015).

[115] ME. REV. STAT. tit. 29-A, § 2117-A(1) (2015).

The California legislature has also placed fairly strict limitations on the California Highway Patrol's use of automatic license plate recognition cameras.[116] The California Vehicle Code states that "[t]he Department of the California Highway Patrol may retain license plate data captured by a license plate reader (LPR) for no more than 60 days, except in circumstances when the data is being used as evidence or for all felonies being investigated . . . ."[117] Furthermore, the California Vehicle Code prohibits the California Highway Patrol from selling automatic license plate recognition data, and it also prohibits sharing of the data with an agency that is not a law enforcement agency or an individual who is not a law enforcement officer.[118] California's legislation requires that the California Highway Patrol to monitor internal use of the data to prevent unauthorized use.[119] In addition to this requirement, the California Highway Patrol is required to report the plate scanner practices and usage, which includes the number of data disclosures, a record of the agencies to which data was disclosed, for what purpose the data was disclosed, and any changes in policy that affect privacy concerns.[120]

Strict regulation of the kind imposed by Maine, New Hampshire, and California provide bright line rules as to what is and what is not permitted when it comes to using automatic license plate recognition systems. However, these bright line tests may come at the expense of law enforcement efficiency. The remaining states appear to have attempted to balance the law enforcement needs with that of protecting citizens' rights by enacting slightly less restrictive rules regarding automatic license plate recognition use.

B. Using Less Strict Legislation to Balance Automatic License Plate Recognition Use and Citizens' Rights

Additional states have enacted less restrictive legislation regarding the use of automatic license plate recognition systems in an attempt to strike a balance between apprehending criminals and protecting citizen's Fourth Amendment rights. Enacted in 2013, an Arkansas statute prohibits the use of automatic license plate recognition cameras by public and private agencies.[121] The statutory exceptions allow automatic license plate recognition cameras to be used by law enforcement for the purposes of an ongoing investigation, by parking enforcement entities for regulating the use of parking facilities, or for the purpose of controlling access to secured areas.[122] Furthermore, Arkansas requires captured license plate data that is not part of an ongoing investigation be deleted within 150 days and prohibits all sharing of the data with other law enforcement agencies unless the captured data indicates evidence of an offense.[123]

---

116 *See* CAL. VEH. CODE § 2413 (West 2015).

117 *Id.* § 2413(b).

118 *Id.* § 2413(c).

119 *Id.* § 2413(d).

120 *Id.* § 2413(e).

121 ARK. CODE ANN. § 12-12-1803 (West 2015).

122 *Id.* § 12-12-1803(b).

123 *Id.* § 12-12-1804(a).

Unique to the Arkansas statute is the requirement that any entity that uses an automatic license plate recognition system allowed under the statute is required to compile statistical data every six months into a format sufficient to allow the general public to review the data.[124] The report must include data representing the number of license plates scanned and the names of the lists against which captured plate data were checked.[125] In addition to this information, for each check of captured license plate data against one of the aforementioned lists the data must also include the number of confirmed matches, the number of matches that upon further investigation did not correlate to an alert, and the number of matches that resulted in arrest and prosecution.[126] Law enforcement agencies required to comply with this rule may find it discouraging and cumbersome, however, it is beneficial to both the agency and the general public nonetheless. Although it may require more work on the part of the agency, it will provide the agency with a significant amount of data regarding the return on investment of these expensive automatic license plate recognition systems. The disclosure of such data to the general public also promotes transparency and may greatly reduce the public's fear of an Orwellian society.[127]

Legislation passed in Utah, using similar language as that of Arkansas, also prohibits the use of automatic license plate recognition cameras, but provides exceptions that are slightly broader than those in the Arkansas statute.[128] For instance, both Arkansas and Utah allow law enforcement officers to use license plate scanners for the purposes of an ongoing investigation, and both states allow parking enforcement entities to use license plate scanners for the purpose of controlling access to secured areas. However, Utah also makes exceptions for the purpose of collecting an electronic toll, for the purpose of enforcing motor carrier laws, and by a public transit district for the purpose of assessing parking needs and conducting a travel pattern analysis.[129] Unlike in Arkansas, government entities in Utah using license plate scanners are not required to compile statistical data[130] and must delete scan data within nine months.[131] The time limit is shortened to thirty days if the data is stored by private entities.[132]

---

[124] *Id.* § 12-12-1805(a)(1).

[125] *Id.* § 12-12-1805(b)(1), (2).

[126] *Id.* § 12-12-1805(b)(3).

[127] Orwell warned of the dangers of mass surveillance through the use of telescreens, which subject citizens to constant surveillance. *See generally* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Signet Classic 1961) (1949). Justice Breyer invoked *1984* in oral argument to describe the dangers of modern surveillance: "no one, at least very rarely, sends human beings to follow people twenty-four hours a day. That occasionally happens. But with the machines, you can. So if you win, you suddenly produce what sounds like 1984." Transcript of Oral Argument at 13, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5360051.

[128] *See* UTAH CODE ANN. § 41-6a-2003 (West 2015).

[129] *Id.* § 41-6a-2003(2).

[130] *Id.* §§ 41-6a-2004(2)(a)-(c).

[131] *Id.* § 41-6a-2004(1)(c).

[132] *Id.* § 41-6a-2005(4)(b).

Vermont legislation requires law enforcement agencies to delete automatic license plate recognition data after eighteen months, it clearly defines who can have access to the data, it defines what circumstances allow a person to access the data, and it requires annual reporting on the use of automatic license plate recognition cameras and data requests.[133] The reporting and oversight required by the statute mandates that the Department of Public Safety establish a review process to ensure that information obtained through use of automatic license plate recognition cameras complies with the statute.[134] The Department of Public Safety is then required to report the results of this review annually to the Vermont Senate and House Committee on Judiciary and on Transportation.[135] The content requirements for these reports are similar to the requirements in the Arkansas and California statutes.[136]

Vermont differs from the other states because its law authorizes a centralized database operated by the Vermont Justice Information Sharing System of the Department of Public Safety.[137] Prior to the enactment of the statute the ACLU of Vermont reported that police departments in all parts of the state were using automatic license plate recognition systems, and that the data was being uploaded to a centralized computer database and retained for four years.[138] Authorizing the use of a centralized database that shares historical data with both in-state and out-of-state law enforcement agencies provides advantages to law enforcement agencies, but the potential to abuse such large databases discussed earlier is still present.[139] For this reason, Vermont has more than cut the storage time in half.[140] Tinkering with the storage time, statistical reporting requirements, and other requirements are ways that states have attempted to balance law enforcement concerns while protecting citizen's rights; however, not every state has attempted to strike such a balance.

C. New Jersey Directive Encourages Widespread Automatic License Plate Recognition System Use

New Jersey's approach is vastly different from the previous statutes. In 2010, the New Jersey Attorney General issued a law enforcement directive promulgating guidelines for the use of automatic license plate recognition cameras.[141] The

---

133 *See* VT. STAT. ANN. tit. 23, § 1607 (West 2015).

134 *Id.* § 1607(e).

135 *Id.*

136 *See id.*

137 *Id.* § 1607(a)(3). The definition section of the statute splits collected data into two categories. The first, or "Active Data," is basically license plate scans that are checked against hot lists. *See id.* § 1607(a)(1). "Historical Data," though, is defined as data collected and "*stored on the statewide ALPR server*." *Id.* § 1607(a)(3) (emphasis added). This statewide server language demonstrates how the Vermont Legislature has authorized the use of a statewide database to facilitate automatic license plate recognition data sharing between local and state agencies.

138 AM. CIV. LIBERTIES UNION, *supra* note 3, at 22.

139 *See id.* at 31.

140 *See* VT. STAT. ANN. tit. 23, § 1607(d)(2) (West 2015).

141 *See* N.J. Att'y Gen., Directive No. 2010-5, *supra* note 11.

directive admits, "that our experience with this new and evolving technology is limited," and purports to restrict the use of automatic license plate recognition cameras for "legitimate law enforcement business."[142] What is drastically different from the statutes previously discussed is that this directive requires that the license plate data be stored for a period of five years, and only allows an agency to delete the data before the five-year period if the data has been transferred to the State Police Regional Operations Intelligence Center or any other system that aggregates and stores data collected by two or more law enforcement agencies in accordance with the provisions set out in the directive.[143] In addition to explicitly authorizing a central database, the directive also explicitly authorizes the sort of data-mining that Justice Sotomayor expressed concern about in her concurring opinion in *Jones*.[144] Under this directive, the data mining is termed "Crime Trend Analysis," which contemplates the use of computer programs to piece together individual scans to track patterns of behavior.[145] The directive does not seem to consider the abuse of such data mining and automatic license plate recognition surveillance practices that have already occurred in major cities around the world.[146] While the New Jersey

---

[142] *Id.* at 2. Exactly what is meant by "legitimate law enforcement business" is unclear but a list of examples expands the definition to include "persons wanted by a law enforcement agency who are of interest in a specific investigation, *whether or not such persons are themselves suspected of criminal activity*." *Id.* at 7 (emphasis added).

[143] *Id.*

[144] *Id.* at 11. Justice Sotomayor warned that, "[t]he Government can store such records and efficiently mine them for information years into the future . . . And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring) (internal citations omitted) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

[145] N.J. Att'y Gen., Directive No. 2010-5, *supra* note 11, at 4 ("'Crime trend analysis' refers to the analytical process by which stored automatic license plate recognition data is used, whether alone or in conjunction with other sources of information, to detect crime patterns by studying and linking common elements of recurring crimes; to predict when and where future crimes may occur; and to link specific vehicles to potential criminal or terrorist activity. The term includes an automated process in which a computer program analyzes stored data to identify potentially suspicious activity or other anomalies involving one or more scanned vehicles and where such automated analysis is done without disclosing personal identifying information about any individual to an authorized user or any other person except as may be authorized . . . .").

[146] *See, e.g.*, Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, ASSOCIATED PRESS (Feb. 23, 2012), http://www.ap.org/Content/AP-In-The-News/2012/Newark-mayor-seeks-probe-of-NYPD-Muslim-spying (describing how New York City police officers reportedly drove unmarked vehicles equipped with automatic license plate recognition cameras around local mosques to record each mosque attendee); Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, THE GUARDIAN (Oct. 25, 2010), http://www.theguardian.com/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance (reporting on more than two hundred automatic license plate recognition systems installed in Muslim suburbs of Birmingham as part of a counterterrorism initiative, but after an investigation by a British newspaper revealed that police had misled residents into believing the cameras were to be used to combat vehicle crime and antisocial behavior, public outrage was so great that the program was cancelled).

directive strikes a bright line rule regarding automatic license plate recognition system use, it does so at the cost of citizens' rights.

D. Virginia's Legislation: the "Active" Versus "Passive" Automatic License Plate Recognition Use Distinction

The Virginia Attorney General's advisory opinion to the Virginia Department of State Police establishes a different approach to automatic license plate recognition system regulation that may be more effective at balancing the competing interests of law enforcement and citizens than the legislation previously discussed. The advisory opinion concludes that the State's Government Data Collection and Dissemination Practices Act prohibits state law enforcement's use of automatic license plate recognition cameras for "passive" data collection, but allows their use for "active" data collection.[147] "Active" collection is when law enforcement collects, evaluates, and analyzes the license plate data in real time to determine the relevance to an ongoing case or emergency. Alternatively, "passive" collection is when law enforcement collects unanalyzed data for potential future use investigating criminal or terroristic activities.[148] Essentially, "passive" collection is collecting and pooling the license plate information of every car that passes by the automatic license plate recognition cameras.[149] Despite the fact that this is an advisory opinion analyzing how automatic license plate recognition cameras fit into current Virginia law, which does not address automatic license plate recognition cameras, it provides a decent framework for potential Ohio legislation regarding automatic license plate recognition systems.

E. Recommendations for the Ohio Legislature Regarding Automatic License Plate Recognition System Regulation

Ohio should look to the other legislation of other states as a guide regarding its own legislation on automatic license plate recognition system regulation. Ohio's legislation on automatic license plate recognition systems should require agencies to report statistical analysis of license plate scan data in a fashion similar to Arkansas. Much like in Arkansas, Ohio agencies should be required to compile statistical data every six months that includes: the number of license plates scanned, the names of the lists against which captured plate data were checked, the number of hot list matches, the number of hot list matches that were incorrect, and the number of matches that resulted in arrest and prosecution. This will aid in holding Ohio law enforcement agencies accountable for automatic license plate recognition use and promote transparency. The statistical analysis will also display the return on investment to both Ohio citizens, whose taxes may be used to pay for these machines, and to agencies that spend time and resources training agents to use them. If the reported number of incorrect matches is high, it would allow agencies to make

---

147 *See* Va. Att'y Gen, Legality of Collection from Automated License Plate Reader, 2013 WL 653025, at *4 (Feb. 13, 2013) (Virginia Attorney General's response to the Superintendent of the Virginia Department of State Police regarding whether the Government Data Collection and Dissemination Practices Act permits law enforcement agencies to collect, maintain, and disseminate LPR data).

148 *Id.* at *1.

149 *Id.* at *3.

changes to their procedures, and it will alert the legislature and privacy advocates that changes need to be made.

My second recommendation is that non-hit license plate scan data be deleted every three weeks unless it is part of an ongoing investigation, in which case it may be retained until the conclusion of the criminal proceedings.[150] Given the factual differences between *Jones*, the Ohio case, and the cases just mentioned, three weeks strikes a balance between the goals of law enforcement and citizens' rights while managing to mesh well with my other recommendations. Further, three weeks would not interfere with the statistical analysis mentioned above since only data representing correct or incorrect matches is required and this data is recorded instantaneously. This data also avoids the potential mosaic theory and data mining problem because it does not require storing the location of the scans but only requires the amount of correct or incorrect scans. In addition, the amount of times that a person passes a police car with a scanner in three weeks is not enough to paint a vivid picture "of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" which was a concern of Justice Sotomayor.[151] This would protect suspicionless citizens while still furthering law enforcement objectives because it allows police to utilize the instantaneous feedback provided by automatic license plate recognition systems to apprehend criminals, while protecting innocent citizens from their data being stored and mined for future intrusions into their daily behaviors.

Much like the other statutes, I would recommend that automatic license plate recognition cameras be permitted to enforce highway tolls, control access to secured areas, and to regulate parking.[152] In these instances, as well as with law enforcement agencies utilizing these scanners, it should be required that the agencies promulgate rules and policies regarding which agency employees have access to the data and the ways in which they are to be trained. These policies should be public information. This would give citizens information regarding who has access to their sensitive information, how they have been trained to handle such information, and how such information is protected.

The last major recommendation I would make is that agencies utilizing this technology be prohibited from sharing or selling the data. This prevents other states or even Ohio agencies from circumventing the statute by sharing data with larger databases and then obtaining access to those databases. These recommendations

---

[150] In a two-and-a-half week GPS tracking instance in which a device was physically placed on a vehicle a state supreme court noted that "when the GPS data was downloaded, it provided a record of every place the vehicle had traveled in the *past.* Sense enhancement devices like binoculars and flashlights do not enable officers to determine what occurred in the past." State v. Jackson, 76 P.3d 217, 223 n.2 (Wash. 2003). The same goes for ALPR Systems—the downloading of such date provides a record of the vehicle's travels, unlike simple sense enhancement devices. Similarly, the New York Court of Appeals addressed a physically attached GPS device over a period of sixty-five days and stated, "It is quite clear that this would not and, indeed, realistically could not have been done without GPS . . . ." People v. Weaver, 909 N.E.2d 1195, 1203 (N.Y. 2009). Once again, ALPR systems go beyond enhancing a law enforcement officer's senses allowing the tracking of citizens without much effort from law enforcement.

[151] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., dissenting).

[152] *See* discussion *supra* Part VI.

regulate the rapidly evolving automatic license plate recognition technologies and prevent law enforcement agencies from performing an end run around unworkable tests created by the courts constitutional interpretation.

CONCLUSION

In drafting Ohio's statutory requirements for the use of automatic license plate recognition cameras, the aforementioned cases and statutes provide a helpful drafting guide for the Ohio Legislature. The Virginia Attorney General's advisory opinion provides an example of the sort of balance the legislature must try to achieve between protecting citizens' Fourth Amendment rights while still providing law enforcement agencies with the technology required to apprehend criminals. The recommendations are not entirely inclusive; however, the areas of automatic license plate recognition regulation they touch on are crucial: how long the data is stored, who has access to such data, how those people have been trained, restrictions on sale of the data, and statistical report requirements to promote transparency and public oversight. These are the areas the legislature must focus on to curb potential abuse of such rapidly changing technological devices.