Hamline Law Review

Volume 38 | Issue 1 Article 5

2015

The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law

Jessica Gutierrez-Alm
Winthrop & Weinstine, Associate Attorney, jalm02@hamline.edu

THE PRIVACIES OF LIFE: AUTOMATIC LICENSE PLATE RECOGNITION IS UNCONSTITUTIONAL UNDER THE MOSAIC THEORY OF FOURTH AMENDMEN PRIVACY LAW

Jessica Gutierrez Alm[*]

[*] J.D., Hamline University School of Law (2014). Jessica is an associate in the patent practice at Winthrop & Weinstine in Minneapolis. Jessica wishes to thank the Hamline Law Review for affording her this opportunity, and for their assistance and professionalism.

I. INTRODUCTION

"In Hitler's Germany and Stalin's Russia, there was very efficient law enforcement, there was very little privacy, and the winds of freedom did not blow."[1] Former Chief Justice Rehnquist recognized that there must be balance between the citizens' right to privacy and the need for safety through government surveillance.[2] In order to find that balance, a compromise between these interests must be reached.[3] As Supreme Court Justice Alito recently remarked in *United States v. Jones*, "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[4] To balance the competing interests of privacy and security, it is the courts' responsibility to apply the Fourth Amendment and ensure that privacy tradeoffs do not reach beyond the bounds of constitutionality.[5]

---

[1] William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 21 (1974).

[2] *See id.* at 2.

[3] *See id.* at 2–3.

[4] United States v. Jones, 132 S.Ct. 945, 962 (2012) (Alito, J., concurring).

[5] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) [hereinafter *Constitutional Myths*] ("[T]he courts must update and redefine the Fourth Amendment as technology evolves, creating and recreating reasonable rules that effectively regulate law

After the terrorist attacks of September 11, 2001, demand for advanced surveillance technologies heightened and government agencies redirected efforts toward preventative surveillance rather than post-crime investigation.[6] As a result of the increased demand, these technologies became increasingly inexpensive and are therefore accessible by local law enforcement agencies.[7] One new surveillance technology currently in use by numerous state and local police departments is Automatic License Plate Recognition (ALPR) software.[8] This technology, which only recently caught the attention of privacy advocates and the press, enables law enforcement to collect information on the whereabouts of every person who owns and drives a vehicle on public roads.[9] The systems use digital cameras to capture images of license plates, which are then recorded along with the time, date, and global positioning system (GPS) coordinates where the plate was spotted.[10] Widespread use of the devices and compilation of the historical data permit officials to track an individual's movements across town and across the country.[11] This close monitoring of daily movements is used widely and without warrants.[12]

The Fourth Amendment, which protects citizens' "reasonable expectation of privacy" by preventing unreasonable searches and seizures, is implicated by such indiscriminate data collection.[13] Although it is well-accepted in Fourth Amendment jurisprudence that there is no reasonable expectation of privacy in a person's travels on public roads, multiple points of location compiled over time may reveal intimate personal details.[14] The

---

enforcement and protect privacy in new technologies. The historical premise suggests that the courts should play an active role in the regulation of new technologies because they have done so successfully in the past").

[6] Courtney E. Walsh, *Surveillance Technology and the Loss of Something a lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 171 (2012); Carla Scherr, *You Better Watch Out, You Better Not Frown, New Video Surveillance Technologies are Already in Town (and Other Public Spaces)*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 499, 500 (2008).

[7] *Id.* Walsh, *supra* note 6 at 171; Scherr, *supra* note 6, at 500.

[8] *See* sources cited *infra* note 31 (surveying the widespread use of ALPR systems throughout United States law enforcement agencies).

[9] *See infra* text accompanying notes 22–64 (explaining operation of ALPR systems and ALPR data compilation practices).

[10] *See infra* text accompanying note 22 (explaining the use of digital cameras in ALPR systems); *infra* text accompanying note 41 (explaining the information that is collected and stored with each ALPR scan).

[11] *See infra* text accompanying notes 22–64 (explaining operation of ALPR systems and ALPR data compilation practices).

[12] *See infra* text accompanying notes 22–64 (explaining operation of ALPR systems and ALPR data compilation practices).

[13] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see infra* text accompanying notes 189–241.

[14] *See infra* text accompanying note 108 (recognizing the *United States v. Knotts* holding that there is no reasonable expectation of privacy in a person's public travels); *infra* text accompanying notes 38–64 (detailing the data collection practices of ALPR systems). Additionally, courts have held that a privacy interest does not exist in license plates. *See*

"mosaic theory," as set forth in *United States v. Maynard* and approved by the *United States v. Jones* concurrences, applies the doctrine of reasonable expectations to compiled location data.[15] When ALPR data on a person's license plate is compiled and examined in a mosaic, it violates the driver's reasonable expectation of privacy and infringes Fourth Amendment protections.[16]

Part II of this article begins with a discussion of the widespread use of ALPR systems and the advanced technological capabilities of the devices.[17] Next is an examination of the United States Supreme Court's development of Fourth Amendment privacy law concepts and the various tests developed to determine the existence of an infringement.[18] Part II concludes with a look at the mosaic theory applied to privacy law, as set forth by the *United States v. Maynard* majority and concurring opinions in *United States v. Jones*.[19] Part III then argues that widespread collection and compilation of ALPR data violates the Fourth Amendment right to privacy under the mosaic basis of analysis.[20] Finally, Part III suggests that, as an alternative to adoption of the mosaic theory, ALPR data collection practices should be regulated by legislatures.[21]

United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989) (citing United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980)).

[15] *See infra* text accompanying notes 131–164 (discussing the application of the mosaic theory to long-term GPS tracking in *United States v. Maynard* and the *United States v. Jones* concurrences); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S.Ct. 945 (2012).

[16] *See infra* text accompanying notes 189–241 (arguing that the collection of multiple ALPR data points over time violates the Fourth Amendment under the mosaic theory approach).

[17] *See infra* text accompanying notes 22–64 (describing the operation of ALPR systems and their current usage throughout the world).

[18] *See infra* text accompanying notes 65–128 (describing Fourth Amendment jurisprudence before and after *Katz*).

[19] *See infra* text accompanying notes 129–188 (discussing the history of the mosaic theory and its application in *Maynard* and *Jones*).

[20] *See infra* text accompanying notes 189–252 (arguing that the collection of multiple ALPR data points over time violates the Fourth Amendment under the mosaic theory approach and that policy dictates such a finding).

[21] *See infra* text accompanying notes 253–267 (arguing the need for regulation of ALPR data collection practices).

II. BACKGROUND

A. ALPR: Digital Cameras Capture Location Data of the Entire Driving Population

ALPR systems use specialized digital cameras to automatically capture images of nearby license plates on moving or parked vehicles.[22] When a license plate passes through the camera's field of view, the camera captures several digital pictures, reading the license plate numbers from the images.[23] The system automatically compares the resulting plate numbers to "hotlists": lists of license plate numbers related to stolen vehicle reports, active arrest warrants, AMBER alerts, parolees, and known sex offenders.[24] If the system registers a match between a hotlist license plate and an image captured, an alert is sent to officers.[25] The ALPR camera systems may be either mobile or stationary. Mobile systems are mounted to the outside of police cruisers and capture images of license plates they pass on the road.[26] Stationary ALPR systems have additional capabilities.[27] They can be used to set up zones or "geo-fences" where sex offenders, parolees, probationers, or others are not permitted to enter or leave.[28] When the stationary cameras register the license plate of a prohibited individual crossing such a restricted boundary, officers are alerted.[29]

The technology was developed in Britain in 1976 and was first used in the 1990s as a defense against Irish Republican Army attacks.[30] Today, ALPR systems are used by numerous law enforcement agencies across the

---

[22] INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 1, 5 (2009) [hereinafter IACP REPORT], *available at* http://www.theiacp.org/portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.

[23] *Id.*

[24] *Id.* at 25–26.

[25] Tyson E. Hubbard, Comment, *Automatic License Plate Recognition: An Exciting New Law Enforcement Tool with Potentially Scary Consequences*, 18 SYRACUSE SCI. & TECH L. REP. 3 (2008).

[26] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 285 (2011).

[27] IACP REPORT, *supra* note 22, at 24.

[28] *Id.;* Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARS TECHNICA (Sept. 27, 2012), http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/2/.

[29] Farivar, *supra* note 28; IACP REPORT, *supra* note 22, at 24.

[30] DAVID J. ROBERTS & MEGHANN CASANOVA, AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS: POLICY AND OPERATIONAL GUIDANCE FOR LAW ENFORCEMENT 1, 5 (2012) (Nat'l Criminal Justice Reference Serv. Document No. 239604), *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf. ALPR, also called Automatic Number Plate Recognition (ANPR), was invented in 1976 by the Police Scientific Development Branch in the United Kingdom. *Id.* Irish Republican Army terrorist bombings in the City of London prompted creation of the "Ring of Steel" in 1993—a surveillance trap, which initially used closed-circuit television cameras. *Id.* ANPR cameras were incorporated into the "Ring of Steel" in 1997. *Id.*

United States, as well as in various countries.[31] In Minnesota, the systems are currently used by the cities of Minneapolis, St. Paul, Bloomington, Lakeville, Maplewood, Washington County, and by the State Patrol.[32] Some stationary systems are even being used in the private sector.[33]

Police use of the systems has been widely successful.[34] The most advanced systems are capable of reading 3,600 license plates per minute, and are capable of reading plates correctly at a "differential speed" of up to 160 miles per hour.[35] Before implementation of ALPR technology, police officers could only check license plates against hotlists by manually typing the numbers into a computer database.[36] While a typical police officer can manually check 50 to 100 license plates during a shift, an ALPR system has

---

[31] *See generally* ROBERTS & CASANOVA, *supra* note 30, at 6–7 (discussing a 2007 Law Enforcement Management and Administrative Statistics survey revealing that of those surveyed, 48% of large (1,001 or more officers) law enforcement agencies regularly used ALPR, 32% of mid-sized (500–1,000 officers) agencies were using ALPR, and 9% of agencies with 51–100 officers were using ALPR. None of the smallest (fewer than 50 officers) agencies that responded reported using the ALPR. A 2011 survey conducted by the Police Executive Research Forum showed that 71% of responding agencies used ALPR, and 85% planned to acquire or increase their use of ALPR within five years); Press Release, SEAG Professional Parking Solutions, V&A Waterfront Leverages SEAG's Improved Efficiencies in Access Control at Africa's Most Visited Tourist Destination (Jan. 4, 2012), http://www.zeag.com/objekt/4/5494ac1c036755db497af021c52cd16b.pdf (discussing ALPR use in South Africa); Farivar, *supra* note 28(discussing ALPR sales in Canada and Mexico); BARRY WATSON & KAREN WALSH, THE ROAD SAFETY IMPLICATIONS OF AUTOMATIC NUMBER PLATE RECOGNITION TECHNOLOGY (ANPR) 1, 3–4 (2008) (discussing ALPR use in Australia and New Zealand), *available at* http://eprints.qut.edu.au/13222/.

[32] Eric Roper, *Police Cameras Quietly Capture License Plates, Collect Data*, STAR TRIBUNE (Aug. 10, 2012) [hereinafter *Police Cameras*], www.startribune.com/local /minneapolis/165680946.html?page=1&c=y.

[33] Farivar, *supra* note 28 (Brigham Young University in Provo, Utah, uses ALPR systems to scan license plates as cars drive onto campus. Santa Monica, California uses the technology to scan plates in parking garages so shoppers can locate lost cars at local shopping malls. The Arden Fair Mall in Sacramento, California uses ALPR systems to scan for stolen cars).

[34] *See* POLICE EXECUTIVE RESEARCH FORUM, CRITICAL ISSUES IN POLICING SERIES: "HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING?" 1, 29–32 (2012) (discussing the benefits of ALPR shown in a study and experienced by various enforcement agencies), *available at* http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf;); ROBERTS & CASANOVA, *supra* note 30, at 23.

[35] *See* PIPS TECHNOLOGY, THE DRIVING FORCE IN AUTOMATIC LICENSE PLATE RECOGNITION (2009) (manufacturer's ALPR brochure), *available at* http://www.unifiedps.com/wpcontent/uploads/2012/06/pips/lit/PIPS_Law_Enforcement_Solutions.pdf

[36] *See* MOTOROLA, SOLUTION BRIEF: AUTOMATIC LICENSE PLATE RECOGNITION (2011) (manufacturer's ALPR brochure), *available at* http://www.motorolasolutions.com/web/Business/Products/Software%20and%20Applications/Public%20Sector%20Applications/Video%20Applications/Automatic%20License%20Plate%20Recognition%20%28ALPR%29/_Documents/Static%20Files/Motorola_ALPR_Solution_Brief.pdf.

the capability of processing at least 5000 license plates in the same amount of time.[37]

B. ALPR Data Collection Practices: Location Data is Compiled into Extensive Data Banks

When used as described above, the ALPR technology enhances police capabilities.[38] It records and checks more license plates against hotlists than a police officer could manually, and permits lawful traffic stops of suspected offenders based on probable cause.[39] However, one feature of the ALPR system is that it compiles and stores the license plate locations it encounters, at least until the data is erased.[40] Each license plate number, along with the date, time, and exact global positioning system (GPS) coordinates where the plate was scanned are recorded in the ALPR's computer database.[41] As one city police chief explained, the "real value" of the ALPR "comes from the long-term investigative uses of being able to track vehicles—where they've been and what they've been doing."[42] There is currently no legal standard or guideline regulating how long this data can be stored; instead, each law enforcement agency uses its discretion.[43] Some agencies do not keep the data on file for long.[44] The Minnesota State Patrol, for example, retains ALPR data for only 48 hours, while the Saint Paul Police Department erases its data after 14 days.[45] Others, the Washington State Police and California Highway Patrol for example, keep the data on file

---

[37] *Id.* In Minneapolis, Minnesota, the police department's ten ALPR readers captured 805,000 plate numbers in June 2012. *Police Cameras*, *supra* note 32. Of those, roughly 6,100 matched hotlist plate numbers. *Id.* When ALPR systems were implemented in Long Beach, California, within six months, 929 lost or stolen vehicles were identified, 275 stolen vehicles were recovered, and 50 arrests were made. MOTOROLA, *supra* note 37. Within thirty days, the same department impounded 300 vehicles and collected over $200,000 in delinquent fines and impound fees with the use of ALPR technology. *Id.*

[38] *See supra* text accompanying notes 34–37 (discussing the positive effects on crime and arrest rates seen with ALPR use).

[39] *See supra* text accompanying notes 34–37. Prior cases have determined that manual checks of license plate numbers are constitutional and when such a check registers a hit with a hotlist, there is probable cause for a lawful stop. *See* United States v. Walraven, 892 F.2d 972 (10th Cir. 1989).

[40] *E.g.*, ROBERTS & CASANOVA, *supra* note 30 at 28.

[41] *Id.*

[42] Brian Alseth, *Automated License Plate Recognition: The Newest Threat to Your Privacy When You Travel*, ACLU BLOG (May 26, 2010, 9:31 AM) (quoting Charlie Beck, Los Angeles Police Dep't Chief of Detectives), http://www.aclu-wa.org/blog/automated-license-plate-recognition-newest-threat-your-privacy-when-you-travel.

[43] IACP REPORT, *supra* note 22, at 37 (recognizing the need for standards and policies for ALPR data retention).

[44] *See Police Cameras*, *supra* note 32 (noting that Maine requires police to erase such data in 21 days unless it is being used for an investigation).

[45] *Police Cameras*, *supra* note 32.

for up to sixty days.[46] The Minneapolis Police Department, Tennessee Highway Patrol, and Maryland State Police Department retain their ALPR data for a full year.[47] The New York State Police Department is currently one of few law enforcement agencies without a limit on its ALPR data retention; they keep the data indefinitely.[48] Retaining the logs of license plate numbers, times, and locations permits police to use the technology retroactively.[49] Police can sort through data that is months or years old to locate vehicles on a certain date at a certain location, or, arguably more concerning, to track the long-term movements of a particular individual.[50]

Additionally, the data from multiple jurisdictions and states is being combined by federal agencies and third-party companies into massive national databases.[51] One company based in California operates what it calls the National Vehicle Location Service: a private database, currently with over 550 million license plate entries collected by the company and submitted by public entities.[52] The database is available for use by law enforcement investigators at no cost.[53] Such an expansive bank of ALPR data permits agencies to broadly track an individual's movements across the country.[54]

While there may be legitimate reasons for tracking an individual's movements over time, ALPR cameras and computers do not distinguish

---

[46] Farivar, *supra* note 28.

[47] *Id. Police Cameras*, *supra* note 32.

[48] Farivar, *supra* note 28.

[49] ROBERTS & CASANOVA, *supra* note 30, at 28.

[50] *See id.*; MOTOROLA, *supra* note 36.

[51] *See infra* text accompanying notes 52–54 (discussing the compilation of ALPR data by federal agencies and third parties).

[52] Farivar, *supra* note 28. The company boasts that it has around 22,000 U.S. law enforcement officers utilizing the system, and around 1,000 more access the system each month. *Id.*

[53] *Id.* While the only identifying information recorded by the ALPR systems is license plate numbers, the plate numbers can be cross-referenced with Department of Motor Vehicles information to determine vehicle owners, and therefore the likely drivers of the vehicles tracked. Since every car must be registered, access to license plate numbers and Department of Motor Vehicle records permits tracking of every individual with a registered vehicle. *See* Cynthia Lum et al., CENTER FOR EVIDENCE-BASED CRIME POLICY, GEORGE MASON UNIVERSITY, LICENSE PLATE RECOGNITION TECHNOLOGY (LPR): IMPACT EVALUATION AND COMMUNITY ASSESSMENT 1, 67 (2010), *available at* http://cebcp.org/wp-content /evidence-based-policing/LPR_FINAL.pdf.

[54] This has piqued the interest of some federal agencies. Immigration and Customs Enforcement recently awarded a contract to the company operating the National Vehicle Location Service to compile a database that would assist with locating fugitive immigrants. Farivar, *supra* note 28. The Department of Homeland Security's Customs and Border Protection and the Drug Enforcement Agency are also reportedly sharing license plate information banks. Andy Greenberg, *U.S. Customs Tracks Millions of License Plates and has Shared Data with Insurance Firms*, FORBES (Aug. 21, 2012), http://www.forbes. com/sites/andygreenberg/2012/08/21/documents-show-u-s-customs-tracking-millions-of-license-plates-and-sharing-data-with-insurance-firms.

criminals from non-criminals.[55] The systems indiscriminately photograph and record the license plates they encounter.[56] This permits law enforcement entities and third parties to track the whereabouts of every person with a registered vehicle in the United States, a fact that has the American Civil Liberties Union and others on edge due to the potential for privacy invasions.[57]

Not only are potential privacy invasions by government entities a concern with ALPR technology, but issues also arise from the federal Freedom of Information Act and similar state laws.[58] With few exceptions, these laws grant citizens the right to access information from government agencies.[59] In at least some states, ALPR data is not within any of the statutory exceptions to what may be requested under the statutes, and therefore ALPR records may be requested from government agencies by any citizen.[60] Broad access to ALPR data by the public has the potential for dangerous consequences.[61]

With ALPR data files open to such wide uses and audiences, there is much potential for abuse stemming from data collection policies.[62] The longer an entity retains ALPR data, and therefore the more location data points that are compiled together into a single database, the more extensively a person's whereabouts may be tracked.[63] Currently, at least two states have enacted legislation that limits state agencies' ALPR data collection practices, but restrictions on data retention practices are the exception.[64]

---

[55] ROBERTS & CASANOVA, *supra* note 30, at 30.

[56] *Id.*

[57] Cade Crockford, *In Massachusets, a Registry of Everywhere You've Ever Driven?*, ACLU (May 15, 2012), https://www.aclu.org/blog/technology-and-liberty/massachusetts-registry-everywhere-youve-ever-driven (characterizing ALPR systems as a "warrantless tracking tool, enabling retroactive surveillance of millions of people"); IACP REPORT, *supra* note 22, at 2.

[58] *See Police Cameras*, *supra* note 32.

[59] *See* UNITED STATES DEPARTMENT OF JUSTICE, FOIA.GOV, http://www.foia.gov (last visited Oct. 20, 2012).

[60] *See Police Cameras*, *supra* note 32 (a local Minnesota reporter requested ALPR data on his own license plate from the Minneapolis Police Department under the Minnesota Open Records Law and received "a list of dates, times, and coordinates of his car that illustrated his daily routine"). After reading that reporter's news story, a Minneapolis business owner used the Minnesota Open Records Law to track and ultimately repossess at least one car he had sold to a customer and on which he had not received payment. Eric Roper, *Man Uses License Plate Data to Repossess Car in Minneapolis*, STAR TRIBUNE (Aug. 30, 2012), http://www.startribune.com/local/blogs/168014676.html.

[61] *See Police Cameras*, *supra* note 32 (noting that Bob Sykora, chief information officer for the Minnesota Board of Public Defense, warned in a June 2012 memo that ALPR location data is public due to open records laws, and therefore could enable "burglars to learn someone's daily routine or ex-spouses to track former partners").

[62] IACP REPORT, *supra* note 22, at 17.

[63] *See supra* text accompanying notes 40–50 (describing the data that is collected and retained by ALPR systems, and how that data is used by police).

[64] Rushin, *supra* note 26, at 286. Maine limits retention of ALPR data to twenty-one days, declares the data as confidential, and does not permit ALPR systems to be used by

C. The "Privacies of Life" are Introduced into Fourth Amendment Jurisprudence

Federal and state law agencies' warrantless use of ALPR technology calls constitutional privacy into question.[65] The Fourth Amendment of the United States Constitution protects privacy interests by preventing unreasonable searches and seizures.[66] While there is no mention of "privacy" within the Amendment text or its legislative history, the concept of privacy is an accepted extension of the Amendment in modern courts.[67] The text provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[68] Recognition of the Amendment's privacy protections was first put forward in *Boyd v. United States*, the Supreme Court's first significant examination of the Fourth Amendment.[69] The Court acknowledged the Amendment's original purpose, which was directed toward British officials' abuse of warrants in colonial times.[70] Thus relying on the inherent rights of private property, the *Boyd* Court found that the Amendment protects "the sanctity of a man's home and the privacies of life," and Fourth Amendment privacy was born.[71]

The text of the Amendment only applies to limit government practices if the practices qualify as a "search" or a "seizure" as those terms have been interpreted.[72] A seizure of property occurs when "there is some meaningful interference with an individual's possessory interest in that

---

citizens. ME. REV. STAT. tit. 29-A, § 2117-A (2009). The New Hampshire statute is more general and actually prohibits the use of surveillance on public highways through the use of GPS. N.H. REV. STAT. ANN. § 236:130 (2011); *see generally* Patricia Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 151–52 (stating that data storage has become increasingly cheap and regulations are the exception rather than the rule).

[65] *See supra* text accompanying notes 38–64 (discussing ALPR data collection practices).

[66] *See* U.S. CONST. amend. IV.

[67] Walsh, *supra* note 6, at 175.

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

[69] Boyd v. United States, 116 U.S. 616 (1886). Fourth Amendment cases were rare during the nineteenth century, partially because the Supreme Court did not have jurisdiction to hear appeals by criminal defendants until 1891. Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945, 952 n.42 (1977). The only case prior to *Boyd* that significantly discussed the Fourth Amendment was *Ex parte Jackson*, 96 U.S. 727 (1877). In that case, the Court said in dictum that letters in the mail could only be opened pursuant to a warrant. *Id.* at 733. The Court suggested that the warrant could not be used for the purpose of examining private letters. *Id.* at 735–36.

[70] *Boyd*, 116 U.S. at 624–26; *see* Walsh, *supra*, note 6, at 176; *see also Constitutional Myths*, *supra* note 5, at 816 ("The Fourth Amendment was enacted largely in response to English cases such as Entick v. Carrington, in which Lord Camden had declared that 'our law holds the property of every man so sacred, that no man can set his foot upon his neighbor's close without his leave'") (quoting 95 Eng. Rep. 807 (K.B. 1765)).

[71] *Boyd*, 116 U.S. at 630.

[72] *See* U.S. CONST. amend. IV.

property," and a seizure of a person occurs "when governmental termination of a person's movement is effected through means intentionally applied."[73] Since property is not physically seized when an ALPR system captures an individual's license plate number and compares it to a hotlist, nor is the driver's movement terminated, it is a search and not a seizure that is at issue.[74]

D. What is a Search? Katz and Reasonable Expectations of Privacy

As Justice Scalia recently pointed out in the majority opinion of *United States v. Jones*, the Fourth Amendment has a close connection to property and "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century."[75] In determining whether a search occurred, early cases focused on whether there was a physical trespass.[76] In one of the earliest cases involving technological surveillance by law enforcement, the Supreme Court ruled in *Olmstead v. United States* that a wiretap on a telephone wire in a public street did not constitute a Fourth Amendment search because there was no physical trespass "upon any property of the defendants."[77] However, as surveillance methods grew progressively more intrusive, the Supreme Court finally diverged from the Fourth Amendment's ties to property law in *Katz v. United States*.[78]

In *Katz*, the Supreme Court declared that the amendment "protects people, not places," and that each person is entitled to a reasonable expectation of privacy.[79] The case involved the FBI's use of a listening device placed outside a public phone booth to record the defendant's side of conversations.[80] Under traditional privacy law, there was no privacy violation due to the absence of a physical trespass.[81] However, the Court recognized the need to reevaluate privacy law in view of emerging technologies and held that the defendant's conversation was constitutionally protected, not because of a "general constitutional 'right to privacy,'" but because the Amendment protects what a person "seeks to preserve as

---

[73] Soldal v. Cook County, Ill., 113 S.Ct. 538, 543 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)) (definition of a search); Brower v. County of Inyo, 489 U.S. 593, 593 (1989) (definition of a seizure).

[74] *See supra* text accompanying notes 22–29 (detailing the operation of ALPR systems).

[75] *Jones*, 132 S.Ct. at 949 (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)); *Constitutional Myths*, *supra* note 5, at 816.

[76] *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 303–06 (1967).

[77] Olmstead v. United States, 277 U.S. 438, 457 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[78] *Katz*, 389 U.S. 347 (1967).

[79] *Id.* at 351–52.

[80] *Id.* at 348.

[81] *Id.* at 350.

private."[82] The Court reasoned that since Katz closed the telephone booth door behind him and placed money into the phone, he was "entitled to assume that the words he utter[ed] into the mouthpiece" were not "broadcast to the world."[83] The Court recognized that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[84]

After *Katz*, the Supreme Court continued to recognize that a physical intrusion is not a necessary element of a Fourth Amendment search and adopted the two-pronged test articulated in Justice Harlan's *Katz* concurrence.[85] The concurrence was an attempt to elaborate and bring clarity to the *Katz* analysis, but produced what has been criticized as an unworkable and circular test.[86] Under this test, the Court will find that a Fourth Amendment search occurred if the police action (1) invaded an individual's "actual (subjective) expectation of privacy," and (2) if that expectation is one that "society is prepared to recognize as 'reasonable.'"[87] The test, therefore, places emphasis on both a subjective and objective examination of the defendant's expectation of privacy.

E. The Supreme Court's Fourth Amendment Considerations of Technological Surveillance Methods after Katz

1. Subjective Intent to Keep Private

The subjective prong of the test hinges on an outward manifestation of privacy concerns: a person must have "exhibited an actual (subjective) expectation of privacy."[88] "[O]bjects, activities, or statements that [a person] exposes to 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[89] Courts' difficulty with the subjective element is in determining what constitutes such a showing of

---

[82] *Id.* at 350–51.

[83] *Katz*, 389 U.S. at 352.

[84] *Id*. at 351.

[85] *Id.* at 361 (Harlan, J., concurring); *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Karo, 468 U.S. 705 (1984); California v. Ciraolo, 476 U.S. 207 (1986).

[86] Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1386–95 (2008) ("[Harlan's test] converted a factual question—had the defendant barred others from access to the information?—into a murky two-part analysis with a quasi-subjective part and a quasi-objective part. It is an analysis that courts have mangled ever since. And for good reason: It is almost impossible to administer"); *see also Kyllo*, 533 U.S. at 34 (applying the *Katz* standard but recognizing that it has often been criticized as circular, subjective, and unpredictable); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) ("those actual (subjective) expectations of privacy that society is prepared to recognize as reasonable bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable" (internal quotations and citations omitted)).

[87] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[88] *Id.*

[89] *Id.* (quotations in original).

privacy.[90] Katz's act of "shut[ting] the door behind him, and pay[ing] the toll" were unequivocal acts of an intent to conceal.[91] Such clear outward manifestations do not necessarily reflect in every expectation of daily privacy.[92] Outward manifestations of a desire for privacy are particularly difficult to identify in the information age, as individuals may hold expectations of privacy in information that does not necessarily exist in a physical form.[93]

2. Objective Reasonable Expectation of Privacy and the Supreme Court's Distinction between Enhancing and Extrasensory Technologies

Regarding the objective element, the Supreme Court has focused its analysis on the intrusiveness of the technologies used by law enforcement to collect the information, drawing distinctions between those methods that merely enhance an officer's natural abilities and technologies that create extrasensory abilities.[94] For example, in *United States v. Caceres*, the Supreme Court held that the Internal Revenue Service's use of a hidden recording device to record conversations with the defendant was not a Fourth Amendment search.[95] The Court reasoned that the recording device did not violate a reasonable expectation of privacy, because it only produced the equivalent of an agent taking notes during or after the conversations and therefore only enhanced the officer's natural abilities.[96] Whether the account of the conversations was based on the agent's memory or on a recorded tape, the result was the same and was not a constitutional violation.[97]

Other surveillance technologies yielded similar results.[98] In *Smith v. Maryland*, the Supreme Court held that use of a pen register to record telephone numbers dialed into a phone is like obtaining the phone numbers

---

[90] Harper, *supra* note 86 at 1386–87.

[91] *Katz*, 389 U.S. at 352.

[92] *See* Harper, *supra* note 86, at 1386–87.

[93] *See* Haley Plourde-Cole, Note, *Back to Katz: Reasonable Expectation of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571, 618 (2010).

[94] *See* Adam Koppel, Note, *Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1070–71 (2010) (survey of post-*Katz* technological surveillance Supreme Court cases); Rushin, *supra*, note 30, at 34 (explaining that the use of "sense-enhancing technology" to conduct a search into a constitutionally protected area is unconstitutional).

[95] United Sates v. Caceres, 440 U.S. 741, 751 (1979).

[96] *Id.* at 750–51; *see also* On Lee v. United States, 343 U.S. 747 (1952) (undercover government agent's use of hidden microphone to record conversations without defendant's knowledge was no more intrusive than "eavesdropping outside an open window" and therefore not a search. The Court also notes that "[t]he use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure").

[97] *Caceres*, 440 U.S. at 750–51.

[98] *See, e.g.*, *Smith*, 442 U.S at 735; Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

from an operator.[99] The technology only made an officer's job more efficient and therefore did not violate the Fourth Amendment.[100] Similarly, in *Dow Chemical Co. v. United States*, the Court considered the Environmental Protection Agency's use of aerial photography to view Dow Chemical's manufacturing plant after the company denied a request for an on-site inspection.[101] The Court held that the surveillance method was constitutional because it merely enhanced human vision.[102]

3. Knotts and Karo: Public Surveillance Cannot Cross the Threshold to the Home

In addition to the extra-sensory distinction, the Supreme Court revealed through *United States v. Knotts* and *United States v. Karo* that there is a reasonable expectation of privacy inside the home, safe from public surveillance.[103] *Knotts and Karo* both involved police use of "beepers," which are radio transmitters that emit weak signals.[104] The signal can be picked up by a radio receiver held within range, allowing police to follow the signal while remaining out of site.[105] In *Knotts*, officers attached a beeper to a container of chloroform and monitored its movement from the manufacturer—where the defendant purchased it—to the defendant's home.[106] The Supreme Court held that the defendant's Fourth Amendment rights were not violated because the use of the beeper technology simply augmented the officers' visual abilities.[107] The technology in *Knotts* only enhanced the police's ability to follow the suspect in plain view on public thoroughfares, where there is "no reasonable expectation of privacy."[108] Although *Knotts* articulated the proposition that public surveillance is acceptable under the Fourth Amendment, the Court reserved the question of continuous, long-term surveillance, stating: "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."[109]

---

[99] *Smith*, 442 U.S. at 744. ("Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy").

[100] *See id.*

[101] *Dow Chemical*, 476 U.S. at 227.

[102] *Id.* at 228.

[103] United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984); *see Constitutional Myths*, *supra* note 5, at 831–37.

[104] *See Knotts*, 460 U.S. at 277; *Karo*, 468 U.S. at 707.

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

[106] *Id.* at 278.

[107] *Id.* at 282.

[108] *Id.* at 281–82.

[109] *Knotts*, 460 U.S. at 283–84. Other courts recognized this limitation of the *Knotts* ruling. *See, e.g.*, United States v. Butts, 729 F.2d 1514, 1518 n.4 (5th Cir. 1984) ("As did the Supreme Court in *Knotts*, we pretermit any ruling on worst-case situations that may involve persistent, extended, or unlimited violations of a warrant's terms"); *Maynard*, 615

In the following year, the *Karo* Court distinguished *Knotts* because the beeper used in *Karo* revealed information about what was inside the home.[110] In *Karo*, officers used a beeper attached to a container of ether to determine whether the container was still inside a home after it had been tracked there.[111] As the *Karo* court pointed out, the police in *Knotts* ceased collecting information from the beeper after it reached its destination.[112] In *Karo*, however, monitoring of the location continued, revealing "a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant."[113] In this way, the technology was being used to give the officers the extrasensory ability to know whether the ether remained in the house or had been moved.[114] Both subjective and objective elements of the *Katz* analysis seemed to rely on the fact that information was collected from within the home, and the court drew a clear distinction on that fact.[115] Together, *Knotts and Karo* stand for the proposition that the threshold of the home is a barrier to warrantless surveillance.[116]

4. Jones and Global Positioning System Tracking: The Court Avoids the Issue by Going Back to the Fourth Amendment's Property Law Roots

The most recent Supreme Court decision considering Fourth Amendment privacy in light of technological surveillance was *United States v. Jones*.[117] In *Jones*, officers placed a GPS device on Jones's vehicle to continuously track his location for twenty-eight days.[118] In the D.C. Circuit Court below, the court found the surveillance of Jones to be a Fourth Amendment violation under the *Katz* analysis.[119] After reserving the question of long-term surveillance in *Knotts*, and with the D.C. Circuit already having conducted the analysis, the Supreme Court was well placed to consider long-

---

F.3d at 556–57 (Noting that he [*Knotts*] Court avoided the question whether prolonged "twenty-four hour surveillance" was a search by limiting its holding to the facts of the case before it.) (quoting *Knotts*, 460 U.S. at 283).

110 *Karo*, 468 U.S. at 707.

111 *Id.* at 708–10.

112 *Id.* at 715.

113 *Id.*

114 *Id.*

115 *See Karo*, 468 at 715. *Kyllo* furthered the in-home distinction created by *Knotts* and *Karo*, determining that thermal imaging of the inside of a home was a Fourth Amendment violation. *See Kyllo*, 533 U.S. 27, 34–40 (2001).

116 *See Knotts*, 460 U.S. 276; *Karo*, 468 U.S. 705; *see Constitutional Myths*, *supra* note 5, at 835 ("At first blush, *Kyllo* and *Karo* may appear to embrace expansive Fourth Amendment protections in new technologies. I think it is more accurate to understand these cases as conservative decisions. They are conservative in that they are trying to retain the very core of traditional Fourth Amendment protections: the protection of information about the home traditionally enforced by property law").

117 *Jones*, 132 S.Ct. at 945.

118 *Id.* at 948.

119 *Maynard*, 615 F.3d at 563.

term surveillance under the *Katz* analysis.[120] However, the majority opinion avoided the issue once again.[121] Rather than follow the *Katz* reasonableness test, and thereby be forced to consider the objective and subjective reasonableness of long-term location data, the Court reverted to the Fourth Amendment's property law roots, finding that the officers' action of placing a GPS device on the defendant's vehicle was a common law trespass and therefore a search.[122] The Court thus affirmed the *Maynard* D.C. Circuit opinion, but on the unexpected grounds of a physical trespass. The opinion was reminiscent of the 1928 case, *Olmstead*, which *Katz* overruled.[123] The Court successfully distinguished *Katz*, *Knotts*, and the majority of technological surveillance cases considering the Fourth Amendment because those cases did not involve a physical trespass.[124]

Despite this resurrection of "18th century tort law," the Court stated that a case of purely technological surveillance would "remain subject to the *Katz* analysis."[125] The Court stated only that such constant technological surveillance of Jones over a four-week period without a physical trespass "*may be* . . . an unconstitutional invasion of privacy," but declined to answer the question.[126] However, concurring opinions written by Justices Sotomayor and Alito did attempt to answer the question, and Justice Alito chastised the Court for relying on old property law, rather than examining the modern issue of technological surveillance.[127] The *Jones* concurrences, as well as the lower court, relied on a form of the "mosaic theory" to suggest that the government's compilation of information over a four-week period invaded the defendant's reasonable expectation of privacy.[128]

F. The Mosaic Theory of Aggregated Data Creates a Privacy Interest in the Whole

The mosaic theory encompasses the idea that individual pieces of otherwise unimportant information, when grouped together, can amount to important intelligence information that requires high-level confidential

---

[120] *See id*. at 557 (discussing the Supreme Court's reservation of the question of constant surveillance in *Knotts*, and that the question was squarely presented in the case of *Maynard*/*Jones*).

[121] *Jones*, 132 S.Ct. at 950 ("[W]e need not address the Government's contentions [that there is no reasonable expectation of privacy in the vehicle's locations on public roads], because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation").

[122] *Id.* at 949.

[123] *Compare Olmstead*, 277 U.S. at 464, *with Jones*, 132 S.Ct. at 949; *see supra* text accompanying note 77 (discussing *Olmstead*).

[124] *Jones*, 132 S.Ct. at 951–52.

[125] *Id.* at 957 (Alito, J., concurring), 953.

[126] *Id.* at 954 (emphasis added).

[127] *See id.* at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

[128] *See id.* at 955–56 (Sotomayor, J., concurring); *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

treatment.[129] The concept has been used by government agencies for decades to justify the need to keep certain information confidential.[130] Prior to *Maynard*, the mosaic theory does not appear to have been applied to Fourth Amendment protections.

1. United States v. Maynard and the Jones Concurrences: Applying the Mosaic Theory to Long-Term Surveillance Data Under Fourth Amendment Privacy Analysis

United States v. Maynard was the D.C. Circuit Court's opinion about the tracking of Jones that was later affirmed *sub nom.* and under different grounds in *Jones*.[131] Before the case was appealed to the Supreme Court, *Maynard* incorporated the mosaic theory into its Fourth Amendment analysis of the government's long-term GPS tracking[132] of Jones and thereby found a privacy violation based on the long-term accumulation of data.[133] The court first determined that *Knotts* did not control because the issue of long-term surveillance was expressly reserved in that case.[134] Thus, the facts surrounding the government's collection of GPS data from Jones's car were just the type of "dragnet" surveillance that the Supreme Court avoided considering in *Knotts*.[135] The *Maynard* court then turned to the *Katz* two-prong Fourth Amendment analysis.[136]

---

[129] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005).

[130] *Id.*; In the midst of the Cold War, use of the theory as a justification expanded, and was expressly adopted in an Executive Order issued by President Reagan 1982 as a type of classified information. Christina E. Wells, *CIA v. Sims: Mosaic Theory and Government Attitude*, 58 ADMIN. L. REV. 845, 857 (2006); Exec. Order No. 12356 § 1.3(b), 47 FR 14874 (1982). For a discussion on the executive order, the Clinton administration's abandonment of the mosaic concept in national security, and further executive treatment of the concept after 9/11, *see* Pozen, *supra* note 129 at 641–58.

[131] *Maynard*, 615 F.3d 544 (D.C. Cir. 2010); *Jones*, 132 S.Ct. 945 (2012). Maynard and Jones were co-conspirators tried together, but the GPS tracking device was placed on Jones's car and relevant only to his case.

[132] While ALPR data relies in part on GPS coordinates, as used in this article, "GPS data" will refer only to continuous location data such as that obtained by the GPS tracking device in *Jones.* "ALPR data" will refer to the intermittent location data collected through the use of multiple ALPR cameras and compiled in a database.

[133] *Maynard*, 615 F.3d at 564. Although, the Supreme Court upheld the decision based not on the mosaic theory, but on trespass law concepts in that the placement of the GPS device on Jones's car was a physical trespass, which violated his Fourth Amendment rights. *See supra* text accompanying notes 117–128 (discussing the Supreme Court's reasoning in *United States v. Jones*).

[134] *Id.* at 557 ("*Knotts* held only that a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end . . ." (internal citations omitted)).

[135] *Id.* at 558; *see Knotts*, 460 U.S. at 283–84.

[136] *Maynard*, 615 F.3d at 558.

In considering whether there was a reasonable expectation of privacy, the court concluded that the whole of Jones's movements over the twenty-eight day period was not actually or constructively exposed to the public, and that there was therefore a reasonable expectation of privacy.[137] The court drew a distinction between "single journey[s]" and the mosaic of several journeys summed up over a length of time.[138] Analogizing to early cases that relied on the mosaic theory to restrict public access to confidential government data, the court held that Jones had a reasonable expectation of privacy "in his movements over the course of a month" and that a reasonable person "expects each of those movements to remain disconnected and anonymous."[139] The court illustrated the mosaic theory's application to a person's movements:

> Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit . . . . [A] single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, [or] an associate of particular individuals or political groups.[140]

With regard to the subjective element of the *Katz* analysis, the court relied on the fact that a person could not realistically record and track all the movements of another.[141] This is an example of what Professor Orin Kerr

---

[137] *Id.* at 559–64.

[138] *Id.* at 562.

[139] *Id.* at 563 (internal quotations omitted).

[140] *Id.* at 562. Julian Sanchez also posed an illustrative hypothetical regarding the mosaic theory as applied to GPS data in his Cato @ Liberty blog. "Alice and Bob are having a romantic affair that, for whatever reason, they prefer to keep secret. One evening before a planned date, Bob stops by the corner pharmacy and—in full view of a shop full of strangers—buys some condoms. He then drives to a restaurant where, again in full view of the other patrons, they have dinner together. They later drive in separate cars back to Alice's house, where the neighbors (if they care to take note) can observe from the presence of the car in the driveway that Alice has an evening guest for several hours. It being a weeknight, Bob then returns home, again by public roads. Now, the point of this little story is . . . that in ordinary life, we often reasonably suppose the privacy or secrecy of certain facts—that Bob and Alice are having an affair—that could *in principle* be inferred from the combination of other facts that are (severally) clearly public, because it would be highly unusual for all of them to be observed by the *same* public." Julian Sanchez, *GPS Tracking and a 'Mosaic Theory' of Government Searches*, CATO@LIBERTY (Aug. 11, 2010, 9:22PM), https://www.cato-at-liberty.org/gps-tracking-and-a-mosaic-theory-of-government-searches/ (emphasis in original).

[141] *See Maynard*, 615 F.3d at 560.

defined as the "probabilistic model" of the subjective element.[142] With this model, a subjective expectation of privacy exists when there is a low likelihood that another person or the police could ascertain the information in question.[143] The court held that the likelihood that another would observe all of the movements captured by the GPS device was "essentially nil."[144]

With *Maynard*, the D.C. Circuit Court introduced a novel idea into the Fourth Amendment context by finding a privacy interest in the aggregate of Jones's actions that would not otherwise exist in each individual movement.[145] While the court affirmed the principle that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection," it determined that the whole of a person's movements over twenty-eight days is not actually exposed to the public.[146] Despite the innovation of *Maynard*, on appeal, the Supreme Court majority in *Jones* declined to consider the theory after it found that this case involved a physical trespass, which made for a simpler Fourth Amendment analysis.[147] However, other concurring justices did examine the mosaic concept in *Jones*.[148]

Justices Sotomayor and Alito each wrote concurring opinions in the *Jones* case.[149] While neither opinion expressly endorsed the mosaic theory of the Fourth Amendment put forth by the lower court, both opinions clearly supported the idea that the sum of GPS data collected on Jones was a Fourth

---

[142] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506 (2007).

[143] *Id.* The probabilistic model of the subjective element was also applied in California v. Ciarolo, 467 U.S. 207 (1986). That case involved aerial surveillance revealing marijuana plants on the defendant's property. The Court held that in an age of regular air travel, the plants were likely to be viewed by others, and therefore the subjective expectation of privacy element was not met. *Ciarolo*, 467 U.S. at 213–14.

[144] *Maynard*, 615 F.3d at 560.

[145] Orin Kerr, *D.C. Circuit Court Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, THE VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM) [hereinafter *D.C. Circuit Introduces*], http://www.volokh.com /2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/. After *Maynard*, but before the *Jones* decision came down, the mosaic concept was applied by courts in other technology cases, such as in cases of police applications seeking to obtain cell site location data from defendants' cell phones under the Stored Communications Act. *Compare* In re Application of the United States, 736 F.Supp.2d 578 (E.D.N.Y. Aug. 27, 2010) (application requesting cell side location data for a period of 58 days required warrant because "cumulative cell-site-location records implicate sufficiently serious protected privacy concerns") *with* In re Application of the United States, No. 11 MC 0113, 2011 WL 579925 (E.D.N.Y. Feb. 16, 2011) (application for a period of 21 days did not require warrant).

[146] *Maynard*, 615 F.3d at 559–60.

[147] *See supra* text accompanying notes 117–128 (discussing the Supreme Court's reasoning in *United States v. Jones*).

[148] *See infra* text accompanying notes 149–164 (discussing Justices Sotomayor's and Alito's concurring opinions in *United States v. Jones*).

[149] *Jones*, 132 S.Ct. at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

Amendment violation.[150] Justice Alito's concurrence, with which Justices Ginsburg, Breyer, and Kagan joined, began by criticizing the majority's use of property law concepts in its Fourth Amendment analysis, and anticipated difficulties with future cases that involve only technological surveillance without physical contact.[151]

Justice Alito's analysis applied the *Katz* test and is reminiscent of the majority opinion in *Maynard*.[152] Alito drew a distinction between "relatively short-term monitoring" and the "long-term monitoring" over a twenty-eight day period of *Jones*.[153] He concluded that society does not expect police or others to "monitor and catalogue every single movement of an individual's car for a very long period."[154] Both subjective and objective elements of the analysis rested on application of the concept of a mosaic of information.[155] Alito also applied the probabilistic model for the subjective element that was used in the lower court.[156] Since Jones's reasonable expectation of privacy was violated, there was a Fourth Amendment search under Alito's analysis.[157]

Finally, Justice Sotomayor set forth a separate concurring opinion in *Jones* that provided for an even more expansive view of Fourth Amendment privacy.[158] Sotomayor agreed with the majority's use of property law concepts, stating that it was a finding based on a "constitutional minimum."[159] Sotomayor also agreed with Alito's opinion that long-term GPS surveillance invades reasonable privacy expectations.[160] She went further, however, and reasoned that even short-term "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."[161] Sotomayor stated that these considerations should be taken into account when considering the

---

[150] Orin Kerr, *What's the Status of the Mosaic Theory After Jones?*, THE VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM) [hereinafter *What's the Status*], http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/; *Walsh*, *supra* note 6, at 223.

[151] *Jones*, 132 S.Ct. at 962–67. (Alito, J., concurring).

[152] *Compare Jones*, 132 S.Ct. at 957–64, *with Maynard*, 615 F.3d at 561–64.

[153] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

[154] *Id.*

[155] *Id.*

[156] *Id.; see supra* text accompanying note 154 (quoting Justice Alito's application of the probabilistic model to the subjective element of the *Katz* analysis in his *Jones* concurrence); *see also What's the Status*, *supra* note 150.

[157] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

[158] *See id.* at 954–55 (Sotomayor, J., concurring).

[159] *Id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor agreed with the majority's "constitutional minimum" because a physical trespass occurred when the police officers placed the GPS tracking device on Jones's vehicle. However, in a future case without such a physical trespass, Justice Sotomayor's opinion suggests that she will be willing to find a Fourth Amendment violation in the aggregation of technological surveillance alone.

[160] *Id.*

[161] *Id.* (citations omitted).

government's look into the "sum of one's public movements," suggesting that she would place emphasis on the degree of privacy of the information obtained, but not necessarily the length of monitoring time as a grounds for violating a reasonable expectation of privacy.[162]

Thus, a total of five Supreme Court justices concurred in a willingness to accept a mosaic theory of Fourth Amendment privacy in the *Jones* case.[163] Despite Justice Scalia's characterization of the mosaic concept as one of "novelty" raising "thorny problems," *Jones* may have set the Court up for a future 5-4 majority holding for mosaic theory Fourth Amendment when a case arises with purely technological surveillance and no physical trespass.[164]

2. The Future of the Mosaic Theory in Fourth Amendment Privacy: United States v. Graham, Criticisms, and Limitations

In one of the first cases to consider technological location data since the *Jones* decision, the federal district court that decided *United States v. Graham* chose not to apply the mosaic concept advocated by the *Jones* concurrences.[165] In *Graham*, the defendant sought to have historical cell site location data suppressed after it was obtained from his cell phone by police.[166] The defendant argued that the historical data obtained in the aggregate revealed patterns and "paint[ed] an intimate picture of [his] whereabouts over an extensive period of time."[167]

The *Graham* court recognized *Maynard*'s introduction of the mosaic theory and that the theory was supported by the concurrences in *Jones*.[168] Despite the court's observation that "a five justice [Supreme Court] majority is willing to accept the principle that government surveillance over time *can* implicate an individual's reasonable expectation of privacy," the *Graham*

---

[162] *Id.* at 956 (Sotomayor, J., concurring).

[163] Justices Sotomayor and Alito wrote the concurring opinions that suggested a mosaic-based analysis, and Justices Ginsburg, Breyer, and Kagan joined in Alito's opinion. *See Jones*, 132 S.Ct. 945.

[164] *See supra* text accompanying notes 149–163 (discussing the two concurring opinions in *Jones*); *supra* note 159 (discussing Justice Sotomayor's agreement with both the majority and Alito's opinion).

[165] United States v. Graham, 846 F.Supp.2d 384 (D. Md. 2012).

[166] *Id.* at 386. When a cell phone is turned on, it constantly communicates and registers with close cell phone towers. By identifying which tower the cell phone registered with at a certain point in time, the user's location can be pinpointed to within less than 200 feet. This information is stored by wireless companies and can be obtained by police under the Stored Communications Act, which requires a lesser showing than a warrant. Walsh, *supra* note 6, at 239.

[167] *Graham*, 846 F.Supp.2d at 387. *Graham* involved two magistrate judge orders for historical cell site information. The first order authorized the release of fourteen days of data containing 1,628 individual cell site location data points, while the second order authorized two hundred twenty-one days and 20,235 individual cell site location data points. *Id.*

[168] *Id.* at 391–94.

court withheld application of the mosaic theory, stating that "the law as it now stands simply does not contemplate a situation whereby traditional surveillance becomes a Fourth Amendment 'search' only after some specific period of time."[169]

In its apprehension to apply the mosaic theory, the *Graham* court noted what is considered one of the major flaws of the theory: "retroactive unconstitutionality." [170] The *Maynard* majority and *Jones* concurrences indicated that a shorter length of GPS monitoring, something shorter than twenty-eight days, would have been permissible under the mosaic theory.[171] Assuming that the first day of monitoring alone would have been permissible, then at the end of the first day, Jones's rights were not violated.[172] When the data later accumulated into a mosaic and revealed detailed information about Jones's life, that first day of data became part of an unconstitutional scheme.[173] The crux of the concept put forth by the opinions is that the mosaic is considered as a whole, with a reasonable expectation of privacy in its entirety.[174] Thus, one piece of data that may be constitutional alone can later become retroactively unconstitutional when it is part of a mosaic.[175]

Critics also note that the *Maynard* and *Jones* opinions supporting the theory did not provide "any formulation for determining the size and scope of a mosaic that would trigger Fourth Amendment scrutiny."[176] This creates an issue of practicality in police work, as well as a new basis of argument for defense attorneys.[177] In conducting surveillance, police would have little guidance as to how long the investigation could go on before all of the data already collected becomes unconstitutional.[178] Previously, the Supreme Court has expressed the need to have clear, definable Fourth Amendment tests that could be practically applied to police work.[179] Carried to its limits,

---

169 *Id.* at 394, 401 (emphasis in original).

170 *Id.* at 402 (quoting *D.C. Cicruit Introduces*, *supra* note 145).

171 *See Maynard*, 615 F.3d at 562; *Jones*, 132 S.Ct at 964 (Alito, J., concurring).

172 *D.C. Circuit Introduces*, *supra* note 145.

173 *Id.*

174 *Id.*

175 *Id.*

176 Walsh, *supra* note 6, at 236 (citing *D.C. Circuit Introduces*, *supra* note 145). However, Justices Alito and Sotomayor did recognize the difficulty of drawing the line of unconstitutionality. *Jones*, 132 S.Ct. at 964 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4 week mark"); *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring) (noting that the elements of the *Katz* analysis may be present in short-term GPS monitoring, as well as long-term GPS monitoring).

177 *D.C. Circuit Introduces*, *supra* note 145.

178 *Id.*

179 *See* New York v. Belton, 453 U.S. 454, 458 (1981) (noting that Fourth Amendment restrictions "ought to be expressed in terms that are readily applicable by the police" instead of terms that "requir[e] the drawing of subtle nuances and hairline distinctions" (quoting Wayne R. LaFave, *"Case-By-Case Adjudication" Versus "Standardized Procedures": The Robinson Dilemma*, 1974 SUP. CT. REV. 127, 141)).

the theory could render entire investigations unconstitutional.[180] Defense attorneys would argue that evidence against their clients was collected as a piece of some larger mosaic.[181] These limitations lead some critics to conclude that the regulation of long-term surveillance is better left to the legislature.[182]

A final critique of the use of mosaic theory by the *Maynard* court and *Jones* concurrences is the disassociation from Fourth Amendment jurisprudence.[183] In order to distinguish the *Knotts* framework, the *Maynard* court relied on the Supreme Court's reservation of "dragnet" surveillance in *Knotts*.[184] Aside from that reservation, *Knotts* held that there is no reasonable expectation of privacy when traveling "in an automobile on public thoroughfares."[185] Critics of *Maynard* and *Jones* believe that this precedent should have been followed, and that all of Jones's public movements were therefore not private. Instead, the *Maynard* court hinged the case on the "dragnet" reservation left by *Knotts*, allowing the court to ignore the public thoroughfares precedent.[186] Critics argue that the dragnet reservation of *Knotts* was actually considered in *Karo*, where in-home beeper surveillance was deemed to infringe on privacy rights, and thus *Maynard* and *Jones* should still have been bound by *Knotts*.[187] Despite these criticisms, however, five justices of the Supreme Court appear ready to embrace the mosaic

---

[180] *D.C. Circuit Introduces*, *supra* note 145.

[181] Walsh, *supra* note 6, at 236.

[182] *See id.* at 237–46; *Constitutional Myths*, *supra* note 5, at 808 ("legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux"); *see also* Orin Kerr, *The Case Against the Mosaic Theory*, USVJONES.COM: HOW TO DEFINE FOURTH AMENDMENT DOCTRINE FOR SEARCHES IN PUBLIC?, http://usvjones.com/2012/06/04/the-case-against-the-mosaic-theory/; *Graham*, 846 F.Supp.2d at 390; *Jones*, 132 S.Ct. at 964 (Alito, J., concurring); *but see* Peter Swire & Erin Murphy, *How to Address "Standardless Discretion" After Jones*, USVJONES.COM: HOW TO DEFINE FOURTH AMENDMENT DOCTRINE FOR SEARCHING IN PUBLIC?, http://usvjones.com/2012/06/04/the-case-against-the-mosaic-theory/ ("Some, most prominently Professor Orin Kerr, have urged courts to defer entirely to legislative and executive action. We have both criticized this approach on a number of grounds, including the public choice obstacles to legislation in this area, the political obligation of the Court to act as a co-equal branch, and the important moral authority carried by the Court's pronouncements").

[183] Walsh, *supra* note 6, at 230–31.

[184] *Maynard*, 615 F.3d at 556.

[185] *Knotts*, 460 U.S. at 281.

[186] Walsh, *supra* note 6, at 230–31; *D.C. Circuit Introduces*, *supra* note 145145; *see supra* text accompanying notes 103–109 (explaining the circuit court's reasoning in *United States v. Maynard*).

[187] Walsh, *supra* note 6, at 230–31; *D.C. Circuit Introduces*, *supra* note 145. Although, some critics of the mosaic theory have actually argued that *Knotts* and its holding that any public surveillance is permissible should be overruled. *From Jones to Drones: How to Define Fourth Amendment Doctrine for Searches in Public*, YOUTUBE at 0:54:18 (July 4, 2012), http://youtu.be/_pGCWZGdq08?t=54m18s (Privacy scholars Marc Blitz, Susan Freiwald, Jim Harper, and Christopher Slobogin suggest that *Knotts* should be overruled).

theory of Fourth Amendment analysis based on *Maynard* and Justices Alito's and Sotomayor's concurring opinions in *Jones*.[188]

III. ANALYSIS

A. The Mosaic Theory of Fourth Amendment Analysis Applies to ALPR Data as it was Applied to GPS Data in Maynard and the Jones Concurrences

ALPR systems collect the GPS coordinates of each license plate they encounter.[189] The information is obtained quietly, without the vehicle driver's knowledge, and without a warrant.[190] Each data point is sent to law enforcement agents individually, but more importantly, the data points are compiled together in databases that are maintained for varying lengths of time.[191] Thus, as with the location data obtained by GPS tracking devices that are attached to vehicles, Fourth Amendment privacy is implicated by the use of ALPR systems.[192] As with GPS practices, it is the long-term collection of data that crosses the privacy threshold of reasonable expectations.[193] Short-term location information likely does not infringe on the driver's reasonable expectation of privacy, because it is an established concept in Fourth Amendment jurisprudence that a person's whereabouts are public.[194] However, a person's whereabouts, recorded and tracked over a long period of time, reveal much about the privacies of life.[195] Under the *Katz* analysis, there is both a subjective and objective expectation of privacy in such long-term collection of a person's otherwise public location data, as documented by ALPR systems, which thus equates to a Fourth Amendment search.[196]

---

[188] *See Jones*, 132 S.Ct. at 954 (Sotomayor, J., concurring); *id.* at 957 (Alito, J., concurring).

[189] *See supra* text accompanying notes 22–29 (describing the operation of ALPR systems).

[190] *See supra* text accompanying notes 22–29 (describing the operation of ALPR systems)

[191] *See supra* text accompanying notes 38–64 (explaining ALPR data collection practices).

[192] *See supra* text accompanying notes 38–64 (explaining ALPR data collection practices).

[193] *See supra* text accompanying notes 131–164 (discussing the *Maynard* court's and *Jones* concurrences' application of the mosaic theory to long-term GPS data).

[194] *See supra* text accompanying note 108 (noting the *Knotts* holding that there is no reasonable expectation of privacy in public travels).

[195] *See supra* note 140 and accompanying text (quoting Justice Sotomayor's discussion of the privacy implications of a mosaic of data).

[196] *See infra* text accompanying notes 197–241 (applying the *Katz* subject and objective tests to the long-term collection of ALPR data and arguing that the elements are satisfied).

1. The Subjective Element: A Mosaic of ALPR Data Satisfies the Probabilistic Model of the Subjective Expectation of Privacy

Looking first to the subjective element, it is difficult to display an intent to keep one's whereabouts private when that information is public by nature.[197] To overcome this requirement of an outward display in the privacy interest in GPS data, the *Maynard* court and *Jones* concurring justices looked both to the mosaic theory of data compilation and Orin Kerr's probabilistic model of the subjective element.[198] The opinions found that although a stranger could easily observe a person's location at any given time, it is highly unlikely that the same stranger could or would observe every movement over a four-week period.[199] Therefore, a subjective expectation of privacy was present in the aggregate of location data over that period.[200] Similarly, there is a subjective expectation of privacy in the accumulation of several data points collected and compiled by ALPR systems over time.[201] Although the ALPR data points are generally intermittent, rather than the constant 24-hour surveillance provided by GPS, the likelihood that a stranger could or would collect a driver's intermittent location points over a period of months or years—depending on how long ALPR data is retained in each jurisdiction—is highly unlikely.[202]

This highlights a distinction between the privacy implications of GPS data and ALPR data.[203] GPS tracking provides constant, uninterrupted monitoring of an individual's whereabouts.[204] Location data picked up by ALPR systems, however, are intermittent and are collected only when a person drives within range of an ALPR camera, or when a cruiser-mounted camera passes by another vehicle.[205] As a result, one month of GPS data is likely more invasive and includes more data points than one month of

---

[197] *See supra* text accompanying notes 88–93 (discussing the subjective element of the *Katz* analysis and the difficulty in expressing a subjective intent to keep something private).

[198] *See supra* text accompanying notes 131–164 (discussing the application of the mosaic theory and Orin Kerr's probabilistic model in *Maynard* and the *Jones* concurrences).

[199] *See supra* text accompanying notes 141–144, 156 (discussing Orin Kerr's probabilistic model and its application in *Maynard* and Justice Alito's *Jones* concurrence).

[200] *See supra* text accompanying notes 141–144, 156 (discussing Orin Kerr's probabilistic model and its application in *Maynard* and Justice Alito's *Jones* concurrence).

[201] *See supra* text accompanying notes 38–64 (describing ALPR data collection practices).

[202] *See supra* text accompanying notes 22–29 (explaining how ALPR systems operate to collect intermittent location data).

[203] *See infra* text accompanying notes 204–205 (describing the distinction in the type of data obtained by GPS and ALPR systems).

[204] *See supra* text accompanying notes 137–139 (discussing the *Maynard* court's characterization of the continuous nature of GPS data).

[205] *See supra* text accompanying notes 22–29 (explaining how ALPR systems operate to collect intermittent location data).

accumulated ALPR data.[206] Crossing the privacy threshold by creating a spectrum of data unlikely observable by a stranger would require a longer accumulation of ALPR data than of GPS data.[207] Though with several months or even years of ALPR data that is either compiled in a single jurisdiction or combined by a national agency, the subjective element will be met through the probabilistic model.[208] It is beyond reasonable expectation that a person could or would intermittently observe a person's whereabouts over months or years.[209] Thus, the subjective element of the *Katz* analysis is met with application of Orin Kerr's probabilistic model, as applied in *Maynard* and the *Jones* concurrences.[210] Of course the more troublesome element of the *Katz* analysis is the objective, requiring an evaluation of what society (and the Court) is prepared to accept as a reasonable expectation of privacy.[211]

2. The Objective Element: Presumptions Weighing Against a Finding of a Reasonable Expectation of Privacy are Overcome when ALPR Data is Compiled into a Mosaic

It has been established that there is no reasonable expectation of privacy in a person's whereabouts in public.[212] The *Maynard* court and *Jones* concurrences both recognized this point.[213] *Knotts* held that the public nature of a person's location on public roads precludes any privacy interest.[214] *Karo* highlighted this point by indicating that the threshold to the home divides what is generally public and private information.[215] Similar to the GPS data collected in *Knotts* and *Maynard/Jones*, ALPR data can only be collected in public places due to the cameras' locations on police cruisers and at

---

[206] *See supra* text accompanying notes 204–205 (describing the distinction in the type of data obtained by GPS and ALPR systems).

[207] *See supra* text accompanying notes 142–143 (describing Orin Kerr's probabilistic model of the *Katz* subjective element).

[208] *See supra* text accompanying notes 38–64 (describing ALPR data collection practices and the potential for abuse when the data is compiled).

[209] *See supra* text accompanying note 154 (quoting Justice Alito's statement that society does not expect their movements to be tracked).

[210] *See supra* text accompanying notes 197–209 (arguing that application of the probabilistic model of the *Katz* subjective element to the case of ALPR data satisfies the element).

[211] *See supra* text accompanying notes 94–116 (discussing the Supreme Court's application of the *Katz* objective element of a reasonable expectation of privacy).

[212] *See supra* text accompanying note 108 (noting the *Knotts* holding that there is no reasonable expectation of privacy in a person's public travels).

[213] *See supra* text accompanying notes 138, 153 (showing that the *Maynard* majority and Justice Alito's concurrence in *Jones* each drew a distinction between short term and long-term monitoring).

[214] *See supra* text accompanying note 108 (noting the *Knotts* holding that there is no reasonable expectation of privacy in a person's public travels).

[215] *See supra* text accompanying notes 103–115 (illustrating the *Knotts* and *Karo* cases).

stationary points on public roads.[216] As with GPS data, there is therefore an initial presumption that the public location data collected by ALPR systems is not subject to a reasonable expectation of privacy; something extra must be shown to evince reasonable expectation.[217]

The Supreme Court's surveillance technology jurisprudence suggests a second initial presumption: surveillance technology is used only to enhance police officers' natural surveillance capabilities and does not provide extrasensory abilities.[218] The Court stated in *Knotts* that a few GPS data points do not amount to a Fourth Amendment search because, when used in that way, the technology only enhances police officers' natural surveillance capabilities. [219] *Maynard*, and later the *Jones* concurrences, seemed to confirm this concept, as each court distinguished the facts of *Knotts*, differentiating the GPS data collected on Jones because it was more extensive.[220] When an ALPR system only captures a person's license plate at a few locations, the technology is only enhancing police officers' ability to observe the vehicle and run the license plate against hotlists manually.[221] To overcome this presumption of a mere ability enhancing technology, a criminal defendant arguing invasion of Fourth Amendment rights would need to show that the technology produced information that would not otherwise be obtainable without the technology.[222]

Both presumptions are overcome when a vast quantity of information is collected and compiled together into a mosaic.[223] As Justice Ginsburg articulated in the *Maynard* majority opinion, ongoing GPS surveillance reveals much about a person's private life.[224] Despite the public

---

[216] *See supra* text accompanying notes 22–29 (explaining how ALPR systems operate to collect license plate data through cameras placed in stationary locations or mounted onto police cruisers).

[217] *See supra* text accompanying notes 212–216 (discussing that ALPR data is similar to GPS data in that it is a collection of public information and therefore presumptively not subject to privacy implication).

[218] *See supra* text accompanying notes 94–102 (outlining the Supreme Court's application of the extra-sensory test in cases of surveillance technology).

[219] *See supra* text accompanying notes 107–108 (discussing the Supreme Court's application of the extra-sensory test in *Knotts*).

[220] *See supra* text accompanying notes 134–136 (quoting the *Maynard* court's distinction of *Knotts*); *supra* text accompanying notes 153–154 (quoting Justice Alito's distinction of *Knotts* in his *Jones* concurrence). Both the *Maynard* court and the *Jones* concurrences seemed to distinguish *Knotts* by relying on the reservation of "dragnet" surveillance methods in *Knotts*.

[221] *See supra* text accompanying notes 94–102 (outlining the Supreme Court's application of the extra-sensory test in cases of surveillance technology).

[222] *See supra* text accompanying notes 94–102 (outlining the Supreme Court's application of the extra-sensory test in cases of surveillance technology).

[223] *See supra* text accompanying notes 131–164 (discussing the application of the mosaic theory in *Maynard* and the *Jones* concurrences to find a Fourth Amendment violation in the accumulation of location data).

[224] *See supra* text accompanying note 140 (quoting Justice Ginsburg's description of how long-term GPS data can reveal private information).

nature inherent in driving on public roads, a person does not reasonably expect each of his movements from place to place over the course of days, weeks, or months to be tracked.[225] As stated above, ALPR data is, on its face, less invasive than GPS data because it is not continuous.[226] However, as the use of ALPR systems grows throughout the nation, the probability of a single license plate being captured by a surveillance unit at least once during every journey increases.[227]

While ALPR technology may not on its face have the capability of painting as clear a picture of private life as GPS tracking does, private habits would still be apparent in the collection of several ALPR data points.[228] Additionally, ALPR data can be easily collected and compiled for a longer period of time than GPS data, because the system does not focus on an individual person and does not require the maintenance of an ongoing GPS device on an individual's vehicle.[229] Extensive ALPR databases that could reveal more information than the twenty-eight days of GPS tracking in *Jones* are already in existence.[230] Law enforcement agencies' compilation and sharing of ALPR data is creating data banks of private information.[231] It is this long-term portrayal of habits and patterns revealed over time that imposes a reasonable expectation of privacy and encroaches into the territory of the extra-sensory.

Additionally, the fact that ALPR systems simultaneously collect location data on the entire driving population furthers the argument for its extrasensory capabilities.[232] This sets ALPR data apart from most other surveillance technologies, including GPS devices, which monitor one targeted person.[233] The *Maynard* court and Justice Alito's *Jones* concurrence focused on the distinction between short-term and long-term GPS monitoring to find an extrasensory ability in the collection of GPS data.[234] Long-term

---

[225] *See supra* text accompanying note 154 (quoting Justice Alito's statement that society does not expect their movements to be tracked).

[226] *See supra* text accompanying notes 203–206 (highlighting the distinction between continuously collected GPS data and intermittently collected ALPR data).

[227] *See supra* note 31 and accompanying text (discussing the usage of ALPR technology throughout the United States and in other countries).

[228] *See supra* text accompanying notes 38–64 (describing ALPR data collection practices and the potential for abuse when the data is compiled).

[229] *See supra* text accompanying notes 22–29 (explaining how ALPR systems operate to collect license plate data through cameras placed in stationary locations or mounted onto police cruisers).

[230] *See supra* text accompanying notes 38–50 (detailing the collection practices of various police jurisdictions, as well as third-party companies).

[231] *See supra* text accompanying notes 38–64 (detailing the collection practices of various police jurisdictions, as well as third-party companies).

[232] *See supra* text accompanying notes 22–29 (describing how ALPR systems function to capture data on every license plate that comes within the camera's field of view).

[233] *See supra* text accompanying notes 117–128 (illustrating the use of a GPS tracking device to record the Jones's movements).

[234] *See supra* text accompanying notes 134–136 (quoting the *Maynard* court's distinction of *Knotts* on the basis of short-term versus long-term tracking); *supra* text

GPS surveillance approaches the extrasensory because, although a law enforcement officer could physically track a suspect for hours or days, it is highly unlikely that he could track the suspect consistently for twenty-eight days.[235] Similarly, one ALPR camera arguably does the same work as an efficient police officer in a parked cruiser, copying down every license plate number she sees.[236] However, it would be nearly impossible for police officers to simultaneously copy down all license plate numbers they encounter, and then compile the information into a large database, charting each license plate's movements.[237] Even if this system of manually observing and running every license plate were a physical possibility, it certainly could not be sustained for any length of time, because it would require the officers' full attention.[238] The vast amount of comprehensive information collected by ALPR systems sets it apart as an extrasensory technology that more easily infringes on Fourth Amendment rights than those technologies that have been deemed as only enhancing officers' capabilities.

Thus, like GPS device data, it is the mosaic of ALPR data points that overcomes the presumptions of no privacy in public places and that it is only an enhancing technology.[239] The mosaic theory of Fourth Amendment analysis presented in *Maynard* and endorsed by the concurring opinions in *Jones* must be employed in the consideration of ALPR data in order to demonstrate a reasonable expectation of privacy.[240] Although the Supreme Court majority was unwilling to accept the theory as a basis for the GPS analysis in the *Jones* decision, policy dictates that the mosaic theory should be adopted for Fourth Amendment analysis of ALPR data.[241]

---

accompanying notes 153–154 (quoting Justice Alito's distinction of *Knotts* in his *Jones* concurrence on the basis of short-term versus long-term tracking).

[235] *See supra* text accompanying notes 137–138.

[236] *See supra* text accompanying notes 141–144, 156 (discussing Orin Kerr's probabilistic model and its application in *Maynard* and Justice Alito's *Jones* concurrence).

[237] *See supra* text accompanying notes 22–50 (explaining the operation of ALPR systems and the data compilation practices).

[238] *See supra* text accompanying notes 22–50 (explaining the operation of ALPR systems and the data compilation practices).

[239] *See supra* text accompanying notes 223–238 (arguing that the mosaic of ALPR data reveals private information and suggests that the technology is extrasensory).

[240] *See supra* text accompanying notes 223–238 (arguing that the mosaic of ALPR data reveals private information and suggests that the technology is extrasensory).

[241] *See supra* text accompanying note 164 (highlighting the *Jones* majority's refusal to adopt the mosaic theory).

B. Policy Dictates that the Mosaic Theory Should be Applied as a Basis for Fourth Amendment Privacy Analysis in the Case of ALPR Data

The Supreme Court avoided taking up the issue of long-term technological surveillance in *Knotts* and *Jones*.[242] Despite the availability of the mosaic concept, the Court seems reluctant to expand the Fourth Amendment's privacy protection so broadly.[243] However, ALPR data collection practices encroach more broadly on the public's sense of privacy than does GPS tracking because, unlike GPS devices, ALPR cameras capture location data indiscriminately on each license plate they encounter.[244] The unfettered use of surveillance tactics on the general public calls for a heightened level of privacy protection.[245] As Justice Sotomayor stated in her *Jones* concurrence, allowing the government to collect "a substantial quantum of intimate information about any person" may "alter the relationship between citizen and government in a way that is inimical to democratic society."[246] If the Court is unwilling to find a reasonable expectation of privacy in the long-term collection of a person's whereabouts, a precedent may be set that there is no reasonable expectation of privacy in anything conducted outside the home.[247]

Additionally, as Justice Alito pointed out in his *Jones* concurrence, not recognizing a reasonable expectation of privacy in a mosaic of location data would lead to inconsistent privacy infringement outcomes.[248] For example, since *Jones* confirmed that the physical trespass analysis of Fourth Amendment law is still valid, a mere few hours of GPS tracking may be considered a Fourth Amendment infringement if the officer physically touched the defendant's car while installing the tracking device.[249] However, without the mosaic theory's application to ALPR data collection, five years' worth of documentation of a defendant's travels across the country, as

---

[242] *See supra* text accompanying note 109 (highlighting the Court's reservation of the long-term surveillance issue in *Knotts*); *supra* text accompanying notes 120–121 (highlighting the Court's reservation of the long-term surveillance issue in *Jones*).

[243] *See supra* text accompanying note 164 (highlighting the *Jones* majority's refusal to adopt the mosaic theory).

[244] *See supra* text accompanying notes 22–29 (explaining how ALPR systems operate to collect location data on every license plate that comes into the camera's field of vision).

[245] *See supra* text accompanying notes 243–244 (discussing the use of ALPR systems on the general public).

[246] *Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring) (internal quotations omitted).

[247] *See* sources cited *supra* note 187 (noting some privacy scholars' implications that the holding in *Knotts* that there is no reasonable expectation of privacy in public travels should be overruled).

[248] *See supra* text accompanying note 151 (quoting Justice Alito's concerns about the majority's reversion to property law in the *Jones* opinion).

[249] *See supra* text accompanying note 151 (quoting Justice Alito's concerns about the majority's reversion to property law in the *Jones* opinion).

collected by various enforcement agencies and then compiled into one database, would not be an infringement of the right to privacy because no physical trespass was involved.[250] The inconsistency demonstrates that technology creates the need for expanding concepts of law.[251] Application of the mosaic theory to Fourth Amendment privacy law would protect the type of privacy implication inherent in modern surveillance practices.[252]

C. Alternatively, Legislative Action Should Restrict the Collection and Compilation Practices of ALPR Data

Legislative action may be a more direct way of combating the privacy implications of widespread ALPR data collection than adoption of the mosaic theory of Fourth Amendment privacy.[253] Since the issue arises not in the use of the systems, but in the compilation of data collected by the systems, restriction on how the data is compiled would solve the problem without the need to expand privacy protections.[254] As Justice Alito stated in Jones, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[255]

Many jurisdictions keep ALPR data on file for months or years, which alone may be enough to violate reasonable privacy interests. Once that data is transferred to another agency or third-party data bank, there is no limit on the length of time that the information may be retained.[256] However, if there were restrictions in place on the length of time that *all* state and federal agencies, as well as third-party companies, can keep ALPR data, the database would not present the detailed image of private life that years' worth of data has the potential to do.[257] Restrictions such as those imposed

---

[250] *See supra* text accompanying note 151 (quoting Justice Alito's concerns about the majority's reversion to property law in the *Jones* opinion).

[251] *See supra* text accompanying note 151 (quoting Justice Alito's concerns about the majority's reversion to property law in the *Jones* opinion).

[252] *See supra* text accompanying notes 242–251 (discussing the need for application of the mosaic theory to Fourth Amendment analysis due to the capability of ALPR to infringe on privacy interests without a physical trespass).

[253] *See supra* note 182 and accompanying text (noting the suggestion of some privacy scholars, the *Graham* court, and Justice Alito in *Jones* that the issue of long-term surveillance may be better left to the legislature). New Hampshire and Maine recognized this fact and have already enacted legislature restricting ALPR data compilation. *See supra* note 64 and accompanying text (describing New Hampshire's and Maine's statutes affecting ALPR data).

[254] *See supra* text accompanying notes 189–241 (arguing that it is the mosaic of ALPR location data that infringes on reasonable expectations of privacy).

[255] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring); see sources cited supra note 182 (noting Justice Alito's suggestion in his Jones concurrence that the issue of long-term surveillance may be better left to the legislature).

[256] *See supra* note 54 (discussing the interest of federal agencies and third-party companies in accumulating ALPR data banks).

[257] *See supra* text accompanying notes 38–54 (discussing the uses of ALPR data banks).

by the State of Maine, which identify ALPR data as confidential and limit the retention time to 21 days should be enacted for every jurisdiction, agency, and company that uses the technology or compiles the results.[258] Since ALPR data is intermittently collected, unlike the continuity of GPS data, 21 days would likely not rise to the level of a Fourth Amendment violation.[259] With only 21 days of data, there would likely be few data points recorded, even if the vehicle was spotted once during every trip.[260] Admittedly, 21 days seems a somewhat arbitrary line to draw. Establishing the point at which the data should be deleted, that is, the point at which the sum of ALPR location data on a person infringes the person's privacy rights, is not easily determined.[261] Maine's 21 day limitation might be an appropriate distinction, but perhaps the data should be kept longer for more in-depth police investigations.[262] Or, with the expanding use of ALPR systems, and therefore the more frequent data points obtained on each journey a driver takes, perhaps the limit should be shortened to seven days or 14 days.[263] Since ALPR data is intermittent, rather than constant like GPS data, perhaps ALPR is best limited by the number of data points collected on a single license plate.[264] Justices Alito and Sotomayor suggested in *Jones* that the line would be difficult to draw with respect to GPS data.[265] They agreed, however, "the line was surely crossed" at four weeks of surveillance.[266] Regardless of where the line is drawn with ALPR data, the most direct

---

[258] ME. REV. STAT. tit. 29-A, § 2117-A (2009); *see supra* note 64 (describing Maine's ALPR data retention statute).

[259] *See supra* text accompanying notes 38–64 (describing ALPR data collection practices and the potential for abuse when the data is compiled); *supra* text accompanying notes 117–128 (illustrating the use of a GPS tracking device to record the Jones's movements).

[260] *See supra* text accompanying note 140 (quoting Justice Ginsburg's description of how long-term GPS data can reveal private information). Twenty-one days of ALPR data, even if one data point per trip were collected, likely would not rise to the level of privacy infringement described by Justice Ginsburg in *Maynard*; *but see* sources cited *supra* note 140 (Julian Sanchez's illustration of the invasiveness of ongoing GPS tracking points to the implication that perhaps only a few location points are needed to reveal a detailed image of a person's private life).

[261] *See supra* text accompanying note 140 (quoting Justice Ginsburg's description of how long-term GPS data can reveal private information). It is difficult to determine just how many ALPR data points would be needed to reach this level of intrusiveness. *See supra* text accompanying notes 170–182 (discussing the difficulties in application of the mosaic theory to surveillance practices).

[262] ME. REV. STAT. tit. 29-A, § 2117-A (2009); *see supra* text accompanying notes 38–54 (discussing the uses of ALPR data banks).

[263] *See supra* note 31 and accompanying text (discussing the usage of ALPR technology throughout the United States and in other countries).

[264] *See supra* text accompanying notes 22–50 (explaining the operation of ALPR systems and the data compilation practices).

[265] *See* sources cited *supra* note 176 (noting Justices Alito's and Sotomayor's acknowledgement of the difficulty with drawing a line on unconstitutionality in the mosaic).

[266] *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

protection of the privacy interest in the mosaic of a driver's long-term location data would be through legislative action.[267]

IV. CONCLUSION

Although the act of capturing license plate data and locations in public places does not by itself violate the Fourth Amendment, the compilation, storage, and referencing of that data collected over the long-term is a search within the meaning of the Fourth Amendment under the mosaic analysis put forth in *Maynard*.[268] Application of the mosaic theory permits the compiled ALPR data to be considered as a whole.[269] The aggregated data satisfies both the subjective and objective expectations of privacy of the *Katz* Fourth Amendment analysis.[270] When *Maynard* was affirmed *sub nom.* in *Jones*, the majority refused to accept the theory, but five justices in concurring opinions expressed a willingness to adopt the theory.[271] The Court is set for a future 5-4 decision in favor of a reasonable expectation of privacy in aggregated location data.[272] Given the current state of Fourth Amendment jurisprudence and the lack of data compilation restrictions, new surveillance technologies such as GPS and ALPR demand application of the mosaic theory.[273] Failure to do so will inevitably lead to inconsistent findings and a strained understanding of reasonable privacy expectations.[274] Alternatively, or perhaps additionally for further precaution, legislatures need to step in and restrict the length of time that ALPR data may be retained.[275] It is only through these devices that former Chief Justice

---

[267] *See supra* text accompanying notes 253–266 (arguing that the issue of ALPR data collection practices is best left to the legislature in order to avoid the accumulation of a mosaic with privacy implications).

[268] *See supra* text accompanying notes 189–252 (arguing that application of the mosaic theory to ALPR data renders the collection of data unconstitutional under the Fourth Amendment).

[269] *See supra* text accompanying notes 129–130 (defining the mosaic theory of aggregated information).

[270] *See supra* text accompanying notes 197–241 (arguing that application of the mosaic theory of Fourth Amendment analysis to ALPR data satisfies the *Katz* test).

[271] *See supra* text accompanying notes 149–163 (discussing the two concurring opinions in *Jones v. United States*); *supra* note 159 (discussing Justice Sotomayor's agreement with both the majority and Alito's opinion).

[272] *See supra* text accompanying note 188 (explaining that the Supreme Court justices who joined the concurrences in *Jones* may make up a future majority in a case with only technological surveillance and no physical trespass).

[273] *See supra* text accompanying notes 242–252 (discussing the policy reasons for adopting the mosaic theory of Fourth Amendment analysis).

[274] *See supra* text accompanying note 151 (quoting Justice Alito's concerns about the majority's reversion to property law in the *Jones* opinion).

[275] *See supra* text accompanying notes 253–267 (proposing that the legislatures should enact restrictions on ALPR data retention in order to preserve privacy).

Rehnquist's balance between citizens' privacy and the state's safety can be achieved.[276]

[276] *See supra* text accompanying notes 1–3 (discussing Justice Rehnquist's application of a balancing test in a 1974 Kansas Law Review article, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*).