SHOULD THE USE OF AUTOMATED LICENSE PLATE READERS CONSTITUTE A SEARCH AFTER *CARPENTER V. UNITED STATES*?

INTRODUCTION

Are our privacy interests implicated when police keep records of each and every time our cars are spotted by automated license plate readers? For many years, police have used automated license plate readers (ALPRs) to, among other things, "determine whether a vehicle was at the scene of a crime, to identify travel patterns, and even to discover vehicles that may be associated with each other."[1] These automated license plate readers are high-speed cameras that can be either stationary, e.g. mounted on street poles, highway overpasses, and the like, or mobile, such as when they are mounted on police cars.[2] ALPRs automatically capture snapshots of all license plates that come within their line of sight, recording simultaneously the location, date, and time of the photograph.[3] All the data collected—at times even including images of cars and passengers—is then uploaded to databases that store the information for extended periods of time, sometimes as long as five years.[4] The data can also be analyzed instantaneously before being stored, such as to determine if the vehicle appears on a "hot list." These "hot lists" catalogue a series of license plates associated with stolen vehicles or vehicles suspected of involvement in a crime.[5] When an automated license plate reader scans any license plate appearing on a "hot list," the police are notified.

At first glance, automated license plate readers may not seem to pose a great threat to privacy interests. After all, they only capture license plate data in individual snapshots. They mark one moment in time, and that seems harmless enough. However, in the aggregate, the pings associated with one license plate can paint a detailed picture of that vehicle and its driver's movements. They can even reveal intimate details about an individual's life

1. *Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/Q7ZH-C575] [hereinafter *Street-Level Surveillance*].

2. *Id.*

3. *Id.*

4. *Id.* Police are not the only collectors of this data, however. Some private companies may retain the data indefinitely. *Id.* These private companies use the data for a variety of purposes, such as processing toll fees and repossessing vehicles. Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC: TECH. (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ [https://perma.cc/7GMN-Y48Q].

5. *Street-Level Surveillance*, *supra* note 1.

as a whole.[6] The stored license plate reader data enables police to make highly accurate estimations regarding individuals' homes, places of work, favorite hangout spots, etc.[7] Police can then infer where an individual will go based on where they have been.[8] What makes this even more troublesome is that drivers *must* display a license plate, allowing automated license plate readers to track the movements of *everyone* in the vicinity, not just those under suspicion of having committed a crime.[9]

Police departments and the government have justified the use of automated license plate readers by stating that the practice occurs in public and is simply a more efficient version of officers recording license plate numbers by hand and entering them into a database.[10] They rely on the

---

6. According to the Electronic Frontier Foundation,

> Taken in the aggregate, ALPR data can paint an intimate portrait of a driver's life and even chill First Amendment protected activity. ALPR technology can be used to target drivers who visit sensitive places such as health centers, immigration clinics, gun shops, union halls, protests, or centers of religious worship.

Id. As one article by the ACLU similarly notes, "[a]utomatic license plate readers (ALPRs) have the ability to capture location data that can reveal details about Americans' religious, sexual, political, medical, and associational activities." Jay Stanley, *Virginia Supreme Court Sees Through Police Claim that License Plate Data Isn't 'Personal'*, ACLU (Apr. 26, 2018, 4:15 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/virginia-supreme-court-sees-through-police-claim-license [https://perma.cc/5XTD-LNHX].

The idea that automated license plate readers can chill associational activities might seem far-fetched, but police officers in New York have been caught targeting Muslims with automated license plate readers. Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics Over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, HUFFPOST (Apr. 25, 2012), https://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html [https://perma.cc/7Y59-8NUS]. One 2012 article includes accounts by former officials who recalled police driving down the street and recording the license plates of all the cars parked in a mosque's vicinity. *Id.*

7. *See* Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from the Cops*, ARS TECHNICA 1 (Mar. 24, 2015, 8:00 AM), https://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/ [https://perma.cc/3CJU-9Z3Q] [hereinafter Farivar, *4.6M Scans*].

8. *Street-Level Surveillance*, *supra* note 1 ("With algorithms applied to the data, the systems can reveal regular travel patterns and predict where a driver may be in the future.").

9. *Id.* ("Drivers have no control over whether their vehicle displays a license plate because the government requires all car, truck, and motorcycle drivers to display license plates in public view. So it's particularly disturbing that automatic license plate readers are used to track and record the movements of millions of ordinary people, even though the overwhelming majority are not connected to a crime.").

10. *See* Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARS TECHNICA 3 (Sept. 27, 2012, 8:30 PM), https://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/3/ [https://perma.cc/MA3T-MRF5] [hereinafter Farivar, *Your Car, Tracked*] ("In 2006, for instance, Gina L. Bianchi, the deputy commissioner and counsel at the New York State Division of Criminal Justice Services wrote in a memo (PDF) to all local law enforcement agencies across the state that there 'does not appear to be any legal impediment to the use of a license plate reader by law enforcement. A license plate reader merely accomplishes, more efficiently, the same task that a police officer may accomplish by reading a license plate and manually entering the number into a database,' she added. 'Therefore, it is reasonable to assume that a court would not hold that the use of a license plate reader would constitute a search.'"). However, one police lieutenant has stated that

general precedent that there is no reasonable expectation of privacy on public thoroughfares.[11] Nevertheless, while the information collected on one occasion is readily available to the public, and a police officer could record it by hand, the accumulation of data points over an extended period of time for an enormous number of drivers is not something the public or the police could easily track.[12] Without automated license plate readers, police officers would be forced to choose what vehicles to monitor.[13] Automated license plate readers, therefore, eliminate the practical limitations on the collection of license plate data that once protected an individual's privacy.[14]

Before the development of automated license plate readers and other new technologies, "our ability to blend into a crowd [served] as sufficient protection" against government invasion of our privacy.[15] The whole of our movements could not be detected. But now, in most communities, we are no longer anonymous individuals in a crowd. Mass data collection methods, such as automated license plate readers, eliminate our anonymity, and the law must adapt to this changing reality. Given the intimate details that automated license plate readers can reveal, we should have a reasonable expectation of privacy with regard to the aggregated information they collect. *Carpenter v. United States*[16] is in line with this assertion.

In *Carpenter*, the Supreme Court examined whether an individual had a reasonable expectation of privacy with regard to cell-site location

automated license plate readers "work[] 100 times better than driving around looking for license plates with our eyes." Dimitar Kostadinov, *Privacy Implications of Automatic License Plate Recognition Technology*, INFOSEC INST. (Feb. 7, 2014), https://resources.infosecinstitute.com/privacy-implications-automatic-license-plate-recognition-technology/#gref [https://perma.cc/LX9X-MLA2].

11. Jessica Gutierrez Alm, *The Privacies of Life: Automatic License Plate Recognition Is Unconstitutional Under the Mosaic Theory of Fourth Amendmen* [sic] *Privacy Law*, 38 HAMLINE L. REV. 127, 129 (2015) ("[I]t is well-accepted in Fourth Amendment jurisprudence that there is no reasonable expectation of privacy in a person's travels on public roads . . . .").

12. *See Street-Level Surveillance*, *supra* note 1. Automated license plate reader data is also frequently shared. Tanvi Misra, *Who's Tracking Your License Plate?*, CITYLAB (Dec. 6, 2018), https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904/ [https://perma.cc/JT4L-B2W7]. This means that the information could be viewed thousands of miles from where it was collected by police in other locales at all levels of government, including, but not limited to, local and state police departments, university campus police, Customs and Border Protection, and Immigration and Customs Enforcement. *Id.*

13. *See Street-Level Surveillance*, *supra* note 1.

14. *Id.*

15. Jake Laperruque, *The* Carpenter *Decision: A Huge Step Forward for Privacy Rights but Major Problems Remain*, PROJECT ON GOV'T OVERSIGHT (June 28, 2018), https://www.pogo.org/analysis/2018/06/carpenter-decision-huge-step-forward-for-privacy-rights-but-major-problems-remain/ [https://perma.cc/6KM7-6ES4].

16. Carpenter v. United States, 138 S. Ct. 2206 (2018).

information[17] cataloguing his movements over a 127-day period.[18] The Court ultimately held that the government's acquisition of Carpenter's cell-site location information constituted a search under the Fourth Amendment and that a search warrant is required to obtain this information.[19] In coming to this conclusion, the Court read its prior decisions as establishing a right to privacy in the whole of an individual's movements.[20] The Court's holding, many commentators believe, calls into question a wide variety of mass data collection methods.[21]

This Note will analyze whether the use of information collected by automated license plate readers should be considered a search under the Fourth Amendment in light of the Court's recent identification of a right to privacy in the whole of an individual's movements. Given that automated license plate readers can reveal so many intimate details about our lives, is there a reasonable expectation of privacy with regard to the use of this information? Should a query of the aggregated data stored for each license plate be considered a search under the Fourth Amendment? Are there sufficient parallels between cell-site location information and automated license plate reader data so that a conclusion similar to that in *Carpenter* will be reached regarding automated license plate readers? This Note will argue that the answer to all of these questions is yes.[22]

---

17. While operating, cell phones connect to radio antennas called "cell-sites." Each time a connection is made, a time-stamped record, known as cell-site location information, is created. *Id.* at 2211. This cell-site location information can be generated via a user's intentional actions or automatically, like when the phone receives a text, and it enables police to pinpoint the individual's location. *Id.* The more cell towers in the area, the more accurately the user's location can be determined. *Id.* Phone companies keep the information for business purposes, but police often acquire the records to reconstruct an individual's movements. Sabrina McCubbin, *Summary: The Supreme Court Rules in* Carpenter v. United States, LAWFARE INST. (June 22, 2018, 2:05 PM), https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states [https://perma.cc/6VLU-56YG].

18. *Carpenter*, 138 S. Ct. at 2212.

19. *Id.* at 2220–21.

20. *Id.* at 2217. The Court also considered the third-party doctrine, which provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)). Despite the importance of the third-party doctrine with regard to privacy rights, the doctrine is outside the scope of this Note.

21. *See* Laperruque, *supra* note 15 ("Achieving the right to privacy in public spaces is likely to have far-reaching implications for emerging surveillance technologies, from facial recognition to automated license plate readers to aerial surveillance. All these technologies threaten to permit dragnet surveillance of our activities and associations on as significant a scale as cellphone location tracking, perhaps even more so. *Carpenter* lays the foundation for challenging unchecked use of these technologies, and makes clear that just because surveillance is of public activities does not mean it can go unchecked."); *see also* Warren Christopher Freiberg, Carpenter v. US*: A Rare Win for Privacy Rights*, TECHNOSKEPTIC (Aug. 31, 2018), https://thetechnoskeptic.com/carpenter-win-privacy/ [https://perma.cc/6W7V-RVB2] ("*Carpenter* also doesn't directly address other types of mass data collection such as automated license plate readers (ALPR), but it does open the door to challenges.").

22. *See infra* Part II.

The Fourth Amendment is meant to protect the public from the overreach of police surveillance and arbitrary power.[23] The government's ability to view pings from automated license plate data collected over an extended period of time, with no detectable check on this power, signifies an overreach of police surveillance. Further, there are identifiable parallels between the collection of cell-site location information and automated license plate reader data, which suggests queries of automated license plate reader data should similarly require a search warrant.[24] Both types of surveillance eliminate the practical limitations police previously faced, which protected individuals against invasions of their privacy.[25] Moreover, automated license plate reader data, while not as constant as cell-site location information, allows the police to gain a thorough understanding of an individual's familial, political, professional, religious, and even sexual associations.[26] Finally, automated license plate reader data, like cell-site location information, is retroactive and involves the collection of information on all individuals and not just those accused of crimes. This means police need not know ahead of time who the target of the investigation will be; everyone is surveilled.[27]

For these reasons, a database query for information on a particular license plate, and therefore the individual driving that vehicle, should be considered a search under the Fourth Amendment. However, a search warrant should not be required for the *collection* of automated license plate reader location data. Even though the existence of these databases can seem troubling, in the interest of not harming law enforcement efforts, police should be permitted to collect license plate information without needing a search warrant.[28] Similarly, there should be an exception to the search warrant requirement for checking vehicles against a "hot list," as this should not be considered a search under the Fourth Amendment.[29] Checking any one license plate at a particular moment would not violate the individual's reasonable expectation of privacy. It is instead the aggregation of license plate data and the inferences that can be made from querying license plate databases that are particularly troubling and therefore should be regulated.[30]

23. *See infra* note 54 and accompanying text.
24. *See infra* Section II.C.
25. *See supra* notes 13–14 and accompanying text; *infra* note 116 and accompanying text.
26. *See supra* notes 6–8 and accompanying text.
27. *See supra* notes 3, 9 and accompanying text; *infra* notes 119–122 and accompanying text.
28. There are certain instances in which automated license plate data could be highly valuable, and it is impossible to go back and collect it after the fact. For this reason, this Note advocates allowing the collection of the data, but regulating its use.
29. *See supra* note 5 and accompanying text.
30. *See supra* notes 6–8 and accompanying text.

Part I of this Note provides additional details regarding the use and implications of automated license plate readers and their data. It also surveys Fourth Amendment jurisprudence leading up to the landmark decision *Carpenter v. United States*. Part II discusses the consequences of *Carpenter* with regard to automated license plate readers and advocates for requiring a search warrant in order to query a database containing automated license plate reader data.

I. BACKGROUND

A. Automated License Plate Readers: A More Detailed Look

As stated in the introduction, automated license plate readers can be either stationary or mobile.[31] When automated license plate readers are mobile, their power is astonishing. The cameras, when mounted on top of squad cars, can capture 1,800 license plates per minute, day or night, enabling one police car to record more than 14,000 plates in a single shift.[32] Often, cameras mounted on squad cars are purposely left on for the entirety of a shift, presumably to capture as much information as possible.[33] Moreover, these cameras can photograph plates even at speeds of sixty-five miles per hour.[34] Therefore, the sheer amount of data the cameras recover is not surprising. One automated license plate reader vendor boasts its database contains over five billion license plate detections with over 150 million more added monthly.[35] Similarly, the Maryland data center shows that automated license plate readers collected eighty-five million reads within the state during 2012 alone.[36]

The percentage of these scans that are linked to criminal behavior, however, is next to nothing. Studies estimate it to be only around 0.2

31. *See supra* note 2 and accompanying text.

32. Jennifer Lynch & Peter Bibring, *Automated License Plate Readers Threaten Our Privacy*, ELECTRONIC FRONTIER FOUND. (May 6, 2013), https://www.eff.org/deeplinks/2013/05/alpr [https://perma.cc/XE9L-CXNG].

33. *See Street-Level Surveillance*, *supra* note 1.

34. Kostadinov, *supra* note 10. One leading license plate reader company claims that its readers can record plates at speeds of 150 miles per hour. Waddell, *supra* note 4.

35. *Platesearch*™, VIGILANT SOLUTIONS, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/ [https://perma.cc/77DW-TCDB].

36. Kostadinov, *supra* note 10. California police might be using automated license plate readers even more aggressively than those in Maryland. Civil litigation revealed the LA Sheriff's Department in conjunction with the LA Police Department has the capability to compile around three million plate scans per week. Robert Miller, *Eyes on the Road: Automatic License Plate Readers*, NAT'L C. FOR DUI DEF., https://ncdd.com/eyes-on-the-road-automatic-license-plate-readers/ [https://perma.cc/T3CV-BWN9].

percent.[37] Using the Maryland data as an example, about one in five hundred scans were hits, and more significantly, "for every one million plates read in Maryland, only [forty-seven] were potentially associated with more serious crimes."[38] That so few scans are connected to crimes is particularly troubling when considering the amount of information that can be learned from the aggregation of license plate data. As previously mentioned, with each snapshot, the readers record the date, time, and location at which the license plate was spotted.[39] Moreover, an entry can even contain images of a car's driver and its passengers.[40] When all of the pings for one license plate are pieced together, police can determine without serious difficulty where an individual lives, works, shops, banks, socializes, etc.[41] In essence, police can discover how we choose to live our lives.

To show how invasive the automated license plate reader technology can be, Ars Technica obtained the automated license plate reader data collected by the Oakland Police Department between December 23, 2010 and May 31, 2014.[42] The dataset for this time period contained 4.6 million reads.[43] After obtaining this information, one Ars Technica reporter sat down with an Oakland city council member.[44] During the meeting, the company accurately determined the block on which the city council member lived within a minute of inquiry, much to the member's surprise.[45]

As automated license plate readers become an increasingly popular tool in the law enforcement toolkit,[46] the information collected will become

37. *Street-Level Surveillance*, *supra* note 1; *see also* Kostadinov, *supra* note 10.

38. Kostadinov, *supra* note 10; *see also* Farivar, *Your Car, Tracked*, *supra* note 10, at 2 ("The New York State Police 2010 Annual Report found that over 57,000 plates were read by the Auto-Theft Unit using its LPRs that year. The result: 200 suspended or revoked registrations . . . and a grand total of three stolen vehicles.").

39. *See supra* note 3 and accompanying text.

40. One California man filed a public record request and discovered 100 images of his car throughout the city, including a photo of "him and his daughters exiting their car while it was parked in their driveway." Kim Zetter, *Even the FBI Had Privacy Concerns on License Plate Readers*, WIRED (May 15, 2015, 8:00 AM), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers/ [https://perma.cc/VDK7-CP8H].

41. *See supra* notes 6–8 and accompanying text.

42. Farivar, *4.6M Scans*, *supra* note 7, at 1.

43. *Id.* Because this time period ended over four years ago, it likely does not accurately approximate the number of reads the database would now contain.

44. *Id.*

45. *Id.* Ars Technica also randomly entered the license plate of a car parked near the bar they were "working" out of into their analytical tool and noted the license plate had been scanned almost 50 times in two clusters: one by the bar and another in a residential neighborhood where the owner presumably lived. *Id.*

46. A 2012 survey by Police Executive Research Forum found that "71 percent of responding agencies use[d the automated license plate reader systems, and] 85 percent . . . plan[ned] on acquiring or increasing their use of LPRs over the next five years." POLICE EXEC. RESEARCH FORUM, CRITICAL ISSUES IN POLICING SERIES: "HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING?" 31 (2012), https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%

more and more invasive. With additional data pings to analyze, greater details can be discerned about individuals' daily lives. As one California state senator aptly noted,

> The thing that I think is not widely understood in the digital age is that there's a difference in degree which ends up being a difference in kind. . . . The ability to collect and maintain data in vast numbers electronically . . . [is] not just a quantitative difference, it's a qualitative difference.[47]

Collecting license plate data by hand and inputting it into a database is simply not the same as using automated license plate readers to perform the same function.[48] Automated license plate readers collect such a large amount of data that the difference is a qualitative one.

As a result, the justification given by police officers and the government for their use is not sufficient.[49] Additional safeguards are necessary to protect our privacy interests. As this Note will argue, a search warrant should be required to query a database for information regarding a particular license plate.[50] That way police are not prevented from collecting this valuable information, but we account for its highly sensitive nature.[51]

20in%20technology%20transforming%20policing%202012.pdf. Similarly, in 2008, Los Angeles Police Department Chief Charlie Beck remarked that automated license plate readers "have 'unlimited potential' as an investigative tool." Lynch & Bibring, *supra* note 32. In the police chief's mind, "the real value comes from the long-term investigative uses of being able to track vehicles—where they've been and what they've been doing—and tie that to crimes that have occurred or that will occur." *Id.*

47. Farivar, *Your Car, Tracked*, *supra* note 10, at 2.

48. As one source states, "[b]y this logic, Big Brother's network of cameras and listening devices in *1984* was merely replacing the old analog technologies of eyes and ears in a more efficient manner, and was really no different from sending around a team of alert humans." Conor Friedersdorf, *An Unprecedented Threat to Privacy*, ATLANTIC: POL. (Jan. 27, 2016), https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/ [https://perma.cc/7J3C-GTY9].

49. Even the FBI was once troubled by the use of automated license plate readers. According to one source,

> Internal documents show that the FBI, based on a recommendation from its own lawyers, was told to stop buying the devices for a time in 2012.
>
> [The documents further demonstrate] the FBI's own Office of General Counsel was grappling with concerns about the agency's use of the technology and the apparent lack of a cohesive government policy to protect the civil liberties of citizens whose vehicles are photographed by the readers.

Zetter, *supra* note 40.

50. *See infra* Part II.

51. This Note's proposed solution does not eliminate the privacy issues associated with misuse of the data, data breach, or inadvertent disclosure. One notable example of data misuse is when a Washington, D.C. police officer pled guilty to extortion in 1998 "after looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners." *Street-Level Surveillance*, *supra* note 1. While at least one police department logs the name of the officer running the query, that department does not require the officer to enter a reason for the search. Even if such a reason were required, officers could easily find a way to circumvent this protection. Farivar, *4.6M Scans*, *supra* note 7, at 3.

B. The Fourth Amendment

The Fourth Amendment of the United States Constitution protects the people against unreasonable searches and seizures.[52] In the Supreme Court's first significant examination of the Fourth Amendment, the Court found that it protects "the sanctity of a man's home and the privacies of life."[53] Further, the Amendment is meant to protect the privacies of life *against* the exertion of "arbitrary power."[54]

Generally, the Supreme Court has held surveillance constitutes a search when it trespasses on property interests or when government action violates the defendant's reasonable expectation of privacy.[55] In these instances, a search warrant is required to ensure the government is not intruding on the privacies of the individual without good reason, or probable cause. The goal is to invade an individual's privacy only when absolutely necessary.

C. Olmstead v. United States*: The Property Rights/Trespass Approach to the Fourth Amendment*

The most famous example of the Court's property rights or trespass approach to the Fourth Amendment is *Olmstead v. United States*.[56] In *Olmstead*, federal officers wiretapped the telephone lines of four residences and one office without a search warrant, thereby intercepting messages that led to the defendants' arrests.[57] In tapping the phone lines, no trespass was made upon the defendants' property.[58] According to the Supreme Court, the absence of a trespass meant no Fourth Amendment search or seizure occurred.[59] In order for there to be a search within the meaning of the Fourth Amendment, there needed to be a physical entry of the defendants' houses or offices.[60] Here there was no "taking away of something tangible," but only "voluntary conversations secretly overheard."[61] The Court reasoned,

---

With regard to inadvertent disclosure, the Electronic Frontier Foundation has investigated several hundred law-enforcement-operated automated license plate readers which were "leaking data because of misconfiguration" and therefore "inadvertently publicly accessible." *Street-Level Surveillance*, *supra* note 1.

52. U.S. CONST. amend. IV.

53. Boyd v. United States, 116 U.S. 616, 630 (1886).

54. *Id.*

55. JOSHUA DRESSLER ET AL., UNDERSTANDING CRIMINAL PROCEDURE, VOLUME 1: INVESTIGATION 66–67 (7th ed. 2017); *see also infra* Sections I.C, I.D, I.E.

56. DRESSLER, *supra* note 55, at 67.

57. Olmstead v. United States, 277 U.S. 438, 456–57 (1928).

58. *Id.* at 457.

59. *Id.* at 464.

60. *Id.*

61. *Id.*

"[t]he Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects."[62] Therefore, the officers' actions did not violate Fourth Amendment protections.[63] Resulting case law focused on constitutionally-protected *areas* and not on the individuals themselves,[64] with the *Olmstead* property rights/trespass approach remaining *the* Fourth Amendment test for thirty-nine years and experiencing a resurgence in recent times.[65]

D. Katz *and* Knotts*: The Reasonable Expectation of Privacy Approach to the Fourth Amendment*

In 1967, the Supreme Court, in the landmark decision *Katz v. United States*,[66] rejected *Olmstead*'s property rights or trespass approach to the Fourth Amendment[67] in favor of a test based on the defendant's reasonable expectation of privacy.[68] In *Katz*, FBI agents attached a recording device to the outside of a telephone booth.[69] The government argued, in line with precedent, that no search occurred as there was no physical entrance into a constitutionally protected area.[70] The Court, however, abandoned this test, declaring that the Fourth Amendment protected "people, not places."[71] According to the Court, what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[72] When Katz entered the telephone booth, he meant to exclude the "uninvited ear."[73] The proper consideration thereafter became whether the defendant's reasonable expectation of privacy was violated;[74] that is, where 1) an individual "exhibited an actual (subjective) expectation of privacy," and 2) the expectation was one that "society is prepared to recognize as 'reasonable.'"[75]

---

62. *Id.*
63. *Id.* at 466.
64. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 301 (1966) ("What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile. There he is protected from unwarranted governmental intrusion." (footnote omitted)).
65. *See infra* notes 67, 82–88 and accompanying text.
66. Katz v. United States, 389 U.S. 347 (1967).
67. *See supra* notes 56–64 and accompanying text.
68. DRESSLER, *supra* note 55, at 66.
69. *Katz*, 389 U.S. at 348.
70. *Id.* at 351.
71. *Id.*
72. *Id.* at 351–52.
73. *Id.* at 352.
74. *Id.* at 361 (Harlan, J., concurring).
75. *Id.* The Court sometimes uses different variants of "reasonable," such as "legitimate" or "justifiable" in its analysis. DRESSLER, *supra* note 55, at 70. Generally, in order for an expectation to be

Following this test, the Court held in *United States v. Knotts*[76] that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[77] In *Knotts*, the police placed a beeper inside a container of chloroform and then tracked the chloroform to the defendant's secluded cabin.[78] In deciding there was no reasonable expectation of privacy, the Court noted that the police could have used visual surveillance to attain the same information provided by the beeper.[79] According to the Court, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[80] However, the Court wisely reserved the question of continuous, long-term surveillance when it stated, "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."[81]

E. United States v. Jones *and the Mosaic Theory*

The Court once again found itself faced with examining the constitutionality of surveillance on public thoroughfares absent a warrant in *United States v. Jones*.[82] In *Jones*, the police tracked the defendant's movements for twenty-eight days using a GPS device planted on his car.[83] In determining whether placing such a device on someone's vehicle and using it to monitor their public movements constituted a search,[84] the Court ultimately returned to its *Olmstead* property rights reasoning.[85] It held that the government had physically intruded on private property and thus conducted a Fourth Amendment search.[86] This holding did not, however,

---

reasonable, it must be "one that an ordinary person might possess" or, in other words, "an expectation of privacy is 'reasonable' when a 'reasonable person' would not expect his privacy is at serious risk." *Id.* at 73.

76. United States v. Knotts, 460 U.S. 276 (1983).
77. *Id.* at 281.
78. *Id.* at 277.
79. *Id.* at 282.
80. *Id.*
81. *Id.* at 284 (emphasis added). The Court's rationale in *Knotts* is that used by the government and police to justify collecting license plate information via automated license plate readers. *See* Lynch & Bibring, *supra* note 32. The government and the police ignore, however, the Court's assertion that dragnet surveillance might call for different constitutional principles.
82. United States v. Jones, 565 U.S. 400 (2012).
83. *Id.* at 403.
84. *Id.* at 402.
85. *See supra* notes 56–64 and accompanying text.
86. *Jones*, 565 U.S. at 404.

reject the *Katz* reasonable expectation of privacy test.[87] Instead, the Court decided that now either test could be used to determine if conduct violated the Fourth Amendment.[88]

Notably, five justices—Sotomayor, Alito, Ginsburg, Breyer, and Kagan—believed that the Court should have instead analyzed the use of the GPS tracking device under the *Katz* reasonable expectation of privacy test and found that the GPS tracker violated the defendant's reasonable expectation of privacy.[89] The concurring justices drew from the lower court's opinion in *United States v. Maynard*,[90] which argued that the whole of Jones's movements was not exposed to the public actually or constructively.[91] According to the court in *Maynard*, "the likelihood anyone will observe all those movements is effectively nil," and "even though each individual movement is exposed . . . that whole reveals more—sometimes a great deal more—than does the sum of its parts."[92] Prolonged surveillance, even in public, the lower court argued, violates an individual's right to privacy because it reveals an intimate picture of the individual's life.[93] As the court aptly noted, "[a] person does not leave his privacy behind when he walks out his front door."[94]

Common in the reasoning of both the lower court in *Maynard* and the *Jones* concurrences is a reliance on the mosaic theory of the Fourth

87. *See id.* at 406–09. According to Justice Scalia,

> [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding. . . . [T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.

Id. (footnote omitted). Therefore, in *Jones*, the Court determined that *Katz* had not really rejected the *Olmstead* approach in favor of the *Katz* approach but rather supplemented it. This conclusion allowed the Court to return to its prior jurisprudence without eliminating the reasonable expectation of privacy approach.

88. DRESSLER, *supra* note 55, at 76.

89. *See Jones*, 565 U.S. at 413–18 (Sotomayor, J., concurring); *Id.* at 418–31 (Alito, J., concurring in the judgment).

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

91. *Id.* at 558.

92. *Id.* The court expanded on these ideas in saying,

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.

Id. at 560. Further, the court noted, "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." *Id.* at 562.

93. *Id.* at 562.

94. *Id.* at 563.

Amendment.[95] The mosaic theory asserts that individually meaningless pieces of information, when aggregated, combine to create a revealing "mosaic," which is far more intrusive than any one piece of information.[96] When viewed all together, the intimate picture painted by the mosaic violates an individual's reasonable expectation of privacy and therefore constitutes a search under the Fourth Amendment. While the *Jones* concurrences do not officially endorse this view, the arguments made by both Justices Sotomayor and Alito support it.

In her *Jones* concurrence, Justice Sotomayor argued the GPS tracking violated the Fourth Amendment because it "reflects a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations."[97] Moreover, the records can be stored and effectively "mined" for years, and the inexpensiveness of GPS monitoring compared to other surveillance techniques, as well as its secrecy, "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[98] Ultimately, Justice Sotomayor seemed skeptical that the average individual would reasonably expect their movements to be recorded and aggregated such that the government could determine "more or less at will, their political and religious beliefs, sexual habits, and so on."[99]

Justice Alito, in his concurrence, echoed these concerns. He argued that in the pre-computer age, individuals were protected by practical limitations on police surveillance: "Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance."[100] GPS tracking, however, eliminated these costs and the protection that they provided. According to Justice Alito, individuals did not expect police to secretly track their every

95. Gutierrez Alm, *supra* note 11, at 142.

96. DRESSLER, *supra* note 55, at 103 ("Just as a mosaic is made up of individual meaningless points that resolve themselves into a meaningful picture when combined together, the mosaic theory holds that aggregating many public pieces of information could result in a 'mosaic' that reveals private information. Thus, even if a person does not have a reasonable expectation of privacy in an individual piece of information (such as one trip along a public road), a person could have a reasonable expectation of privacy in all of his trips along public roads over an extended period. By aggregating all of these individual trips, the police are able to spot patterns and potentially deduce intimate information about the suspect that they would not be able to deduce after monitoring one trip.").

97. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

98. *Id.* at 416 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

99. *Id.*

100. *Id.* at 429 (Alito, J., concurring in the judgment).

movement over an extended period of time, and therefore doing so violated the Fourth Amendment.[101]

F. Carpenter v. United States*: A New Era in Privacy Rights*

Most recently, in *Carpenter v. United States*,[102] the Court decided whether the government violated the Fourth Amendment by accessing, without a search warrant, historical cell-site location information that provided a comprehensive picture of an individual's movements.[103] In *Carpenter*, the police obtained, via court order, cell-site location information spanning a period of 127 days.[104] In analyzing whether the acquisition of this information constituted a search, the Court rejected an argument based on *Knotts*[105] that Carpenter had no reasonable expectation of privacy in his public movements.[106] More specifically, it noted that the Court in *Knotts* "was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance."[107] Ultimately, the Court determined the government had conducted a Fourth Amendment search and that a search warrant must be obtained in order to acquire cell-site location information.[108] In reaching this conclusion, the Court re-examined the underlying principles behind the Fourth Amendment and carefully considered prior precedent in light of technological advances.[109]

According to the Court, previous cases recognized the main goal of the Fourth Amendment as being "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[110] Moreover, the Framers intended "to place obstacles in the way of a too

101. *Id.* at 430.
102. Carpenter v. United States, 138 S. Ct. 2206 (2018).
103. *Id.* at 2211.
104. *Id.* at 2212.
105. *See supra* notes 76–81 and accompanying text.
106. *Carpenter*, 138 S. Ct. at 2219. The Court analyzed the constitutional issue using the reasonable expectation of privacy framework rather than the trespass/property rights view, as there was no physical intrusion. As it stands, the property rights view may rarely be implicated in "the age of 'big data' where all sorts of information can be learned about an individual without any physical intrusion." Lynn R. Fiorentino et al., *The Future of* Carpenter*: Kavanaugh's Privacy Views May Help the Government, But Hinder Individual Privacy Protections, Including Those Accused of Crimes*, ARENT FOX (July 25, 2018), https://www.arentfox.com/perspectives/alerts/future-carpenter-kavanaughs-privacy-views-may-help-government-hinder-individual [https://perma.cc/9QZZ-FQLU].
107. *Carpenter*, 138 S. Ct. at 2215; *see also supra* note 81 and accompanying text.
108. *Carpenter*, 138 S. Ct. at 2221.
109. *See id.* at 2213–18.
110. *Id.* at 2213 (quoting Camara v. Mun. Court of City and Cty. of S.F., 387 U.S. 523, 528 (1967)).

permeating police surveillance."[111] With this in mind, the Supreme Court, echoing the *Maynard* court, declared that individuals do not abandon "Fourth Amendment protection by venturing into the public sphere."[112] Instead, the Court reasoned that a majority had already recognized a "reasonable expectation of privacy in the whole of [an individual's] physical movements."[113] That the movements were in public did not change the fact that an individual was entitled to protection from "too permeating police surveillance."[114]

Some of the key features of cell-site location information particularly troubled the Court.[115] First, like in *Jones*, the Court noted the absence of practical limitations that had previously prevented the government from obtaining such detailed information.[116] Second, the Court noted that cell-site location information amounted to a full accounting of all the individual's whereabouts and therefore provided "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[117] In the Court's assessment, the location records revealed the "privacies of life."[118] Finally, the Court worried about the retrospective nature of the records that not only covered those under suspicion of a crime, but everyone.[119] The Court distinguished the case from that in *Jones* where the police needed to know who the target was first in order to follow him.[120] With cell-site location information, the government could retrace anyone's steps.[121] According to the Court, "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."[122]

In light of the consequences of cell-site location information, the Court declared that its acquisition violates individuals' reasonable expectation of

111. *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

112. *Id.* at 2217; *see also* note 94 and accompanying text.

113. *Carpenter*, 138 S. Ct. at 2217 (first citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment); and then citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see supra* notes 97–101 and accompanying text.

114. *Carpenter*, 138 S. Ct. at 2214 (quoting *Di Re*, 332 U.S. at 595).

115. *See id.* at 2216–19.

116. *Id.* at 2217 ("Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.'" (quoting *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment))); *see also supra* notes 98, 100 and accompanying text.

117. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

118. *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014).

119. *Id.* at 2218 ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection.").

120. *Id.*

121. *Id.*

122. *Id.*

privacy.[123] More significantly, the Court proclaimed that it must consider the consequences of any rule in light of all the new sophisticated systems.[124] It is these consequences that must color our understanding of when there exists a reasonable expectation of privacy.

II. ANALYSIS/PROPOSAL: WHY QUERYING AUTOMATED LICENSE PLATE READER DATA SHOULD REQUIRE A SEARCH WARRANT AFTER *CARPENTER*

A. The Implications of Carpenter v. United States

While the Court once again did not officially endorse the mosaic theory of the Fourth Amendment[125] in *Carpenter*, the theory is implicated by the Court's reasoning. The Court in *Carpenter* recognized that most public actions are not protected under the Fourth Amendment. However, the Court also acknowledged that continued surveillance provides greater details than surveillance of any individual moment alone, and, together, these moments reveal the privacies of life. Consequently, these moments must be protected. It is not enough to say that individuals are protected because some inferences must still be drawn from the information in order to glean fully the details of an individual's life; the Court in *Carpenter* noted its previous rejection of the argument that "inference insulates a search."[126] Therefore, even if the mosaic theory should not be thought of as a test for whether a government action violated the Fourth Amendment, it does hold value as a useful thought experiment, one that can help the Court to understand when an individual's reasonable expectation of privacy has been violated.[127] The government has been using the mosaic theory for decades to justify keeping information hidden from the public;[128] why should the theory not be used to protect individuals as well?

---

123. *Id.* at 2221.

124. *Id.* at 2218.

125. *See supra* note 96 and accompanying text.

126. *Carpenter*, 138 S. Ct. at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

127. This Note does not advocate for the Supreme Court formally adopting the mosaic theory as the proper test for establishing violations of the Fourth Amendment. Using the theory as a test as opposed to as a useful thought experiment poses a variety of problems. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012). Kerr acknowledges the concerns leading courts to support the mosaic theory but urges them to reject the theory as a "dramatic departure" which would require courts to grapple with novel and difficult questions. *Id.* at 311. According to Kerr, these questions include: 1) "What test determines when a mosaic has been created?", 2) "Which surveillance methods prompt a mosaic approach?", 3) "[H]ow [should courts] analyze the reasonableness of mosaic searches[?]", and 4) "[W]hat remedies should apply to unconstitutional mosaic searches[?]". *See id.* at 329.

128. *See* Gutierrez Alm, *supra* note 11, at 143. The government's argument in the national security context is that otherwise insignificant information when put together can become highly confidential intelligence information, or, in other words, seemingly trivial information might be dangerous if it fell

The Court's holding in *Carpenter* that individuals have a reasonable expectation of privacy in the whole of their physical movements, and that some surveillance techniques are simply too invasive, calls into question a variety of surveillance methods.[129] While styled as narrow,[130] the Court's holding suggests that a difference in degree really is a difference in kind.[131] Further, the fact that these new technologies exist, and the public is becoming aware of their existence, does not mean that our privacy rights somehow weaken.[132] Surveillance does not suddenly become permissible because individuals are informed of the fact that the government might be watching. The government cannot argue that certain surveillance methods do not require a search warrant because the expectation of privacy was unreasonable in light of the general awareness of the surveillance.

B. Search Warrants: A Delicate Balancing Act

In order to protect our privacy interests, the use of information collected by new technologies that can, in the aggregate, reveal an intimate picture of an individual's life should require a search warrant. Requiring a search warrant serves as a "bulwark against overreach."[133] As the Supreme Court has noted, "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[134] Rather, search warrants and the rule of probable cause together signify "the best

---

into the hands of, for instance, a hostile intelligence agency. Christina E. Wells, CIA v. Sims*: Mosaic Theory and Government Attitude*, 58 ADMIN. L. REV. 845, 846 (2006). By relying on this version of the mosaic theory, the government has been able to withhold information in the face of Freedom of Information Act ("FOIA") requests. *Id.*

129. *See* Laperruque, *supra* note 15 ("Traditionally information that the government could freely see was by nature not private, and not entitled to Fourth Amendment protections. But by saying that some surveillance power is simply too powerful to exist unchecked in a democracy, the Court upended this idea."); *see also supra* note 21 and accompanying text.

130. *Carpenter*, 138 S. Ct. at 2220.

131. *See* Laperruque, *supra* note 15 ("Although some information may be freely visible to observe and catalog on an individual scale, we're entering a new era where for the first time technology may allow the government to stockpile such data en masse. *Carpenter* established that at some point scale of collection matters more than availability of information on an individual basis.").

132. *See Carpenter*, 138 S. Ct. at 2223 ("[T]he Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." (second alteration in original) (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting))); *see also* United States v. Davis, 785 F.3d 498, 524–25 (11th Cir. 2015) (Rosenbaum, J., concurring) ("[O]ur historical expectations of privacy do not change or somehow weaken simply because we now happen to use modern technology to engage in activities in which we have historically maintained protected privacy interests.").

133. Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 581 (2017).

134. *Id.* (quoting Riley v. California, 573 U.S. 373, 401 (2014)).

compromise that has been found" in the effort to balance both "safeguard[ing] citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime" and "giv[ing] fair leeway for enforcing the law in the community's protection."[135] At its core, the search warrant requirement is a delicate balancing act, carefully considered and designed to both protect individuals' privacy and the government's interest in security.

C. The Parallels Between Cell-Site Location Information and Automated License Plate Reader Data

There are sufficient parallels between cell-site location information and automated license plate reader data to argue that automated license plate readers too should require a search warrant. Like cell-site location information, automated license plate readers pose a substantial privacy risk when their data is examined in the aggregate. First, both cell-site location information and automated license plate readers eliminate the practical limitations that police used to face when deciding to conduct surveillance.[136] Automated license plate readers are not simply a more efficient method of recording license plate numbers by hand and entering them into a database.[137] Without them, police officers would be forced to target specific individuals in order to see where they went on a daily basis. Further, many more personnel would be required, and each officer would have to be paid. Thus, automated license plate readers enable the government at comparatively low cost to determine where individuals habitually go, and the data reveals their patterns, often over the course of several years.

Second, both cell-site location information and data obtained from automated license plate readers can allow police to gain a thorough understanding of an individual's familial, political, professional, religious, and sexual associations.[138] These intimate details are revealed when the information is considered in the aggregate. By examining everywhere a vehicle has been spotted, police can make highly accurate estimations regarding an individual's home, office, grocery store, gym, and so on. Knowing that police can obtain this information might chill certain behavior, such as participation in political protests.[139]

---

135. DRESSLER, *supra* note 55, at 121 (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)).

136. *See supra* notes 13–14, 116 and accompanying text.

137. *See supra* notes 10, 47–48 and accompanying text.

138. *See supra* notes 6–8, 117 and accompanying text.

139. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

Finally, both cell-site location information and information uncovered via automated license plate readers allow officers to retroactively target *anyone*.[140] All drivers are required by law to display a license plate,[141] and automated license plate readers take snapshots of all vehicles that pass in their vicinity, not only those vehicles associated with a crime.[142] In fact, very few vehicles recorded are linked to criminal behavior.[143] Police need not know ahead of time about whom they wish to collect information. The information is simply sitting in a database, waiting for police to ping a license plate and see everywhere the vehicle has been.

While automated license plate data is not as constant as cell-site location information, the information gleaned from it is no less troublesome. We used to be able to blend into the crowd and trust that the whole of our movements could not be detected, but sweeping electronic technologies have eliminated this protection in many communities.[144] A single query of the data collected by automated license plate readers removes our anonymity by detailing those places we most like to visit in one fell swoop. Consequently, a search warrant should be required for a database query regarding information on a particular license plate.

However, in the interest of not harming law enforcement efforts, a search warrant should not be required for the *collection* of automated license plate reader data even though the existence of these databases can seem troubling. Similarly, there should be an exception to the search warrant requirement for checking vehicles against a "hot list," as this should not be considered a search under the Fourth Amendment;[145] checking any one license plate at a particular moment would not violate the individual's reasonable expectation of privacy. It is instead the aggregation of license plate data and the inferences that can be made from it that are particularly troubling and therefore should be regulated.[146]

D. The Need for Constitutional Interpretation Rather than Statutory Regulation

Some commentators argue that statutory regulation rather than constitutional interpretation is the best method to protect against the privacy

140. *See supra* notes 3, 9, 119–122 and accompanying text.
141. *See supra* note 9 and accompanying text.
142. *See supra* note 9 and accompanying text.
143. *See supra* notes 37–38 and accompanying text.
144. *See supra* note 15 and accompanying text.
145. *See supra* note 5 and accompanying text.
146. *See supra* notes 6–8 and accompanying text.

invasions created by new surveillance methods.[147] Constitutional interpretation of the Fourth Amendment, however, is superior to statutory regulation. Though some argue that Congress has certain "institutional advantages,"[148] which might make it appear better suited to address privacy issues raised by new technologies, these institutional advantages rarely come to fruition. For example, Congress can theoretically act quickly when it so chooses,[149] but it rarely does. This is especially true when disagreements exist along party lines.[150]

Further, Congress is fickle; a measure passed by one party may be quickly repealed when the opposing party comes to power following an election. Privacy interests should not be subject to the ebb and flow of political majorities. Similarly, such important protections should not be left to the discretion of state legislatures, which are subject to the same political pressures as Congress and have thus far been ineffective at enacting the necessary safeguards. In 2017, twenty states considered bills related to automated license plate readers, but ultimately none were enacted.[151]

Finally, lawmakers are not always properly motivated to implement automated license plate reader legislation. It has been deemed "politically difficult" for legislators to advocate against law enforcement technologies, such as automated license plate readers, as the public's "kneejerk reaction" is that the automated license plate readers pose no problems if individuals have nothing to hide.[152] While public sentiments might be changing in the

147. *See, e.g.*, Kerr, *supra* note 127, at 350.

148. *Id.*

149. *Id.*

150. Even when one party controls the House of Representatives, the Senate, *and* the White House, that party can be incapable of reaching an agreement. Take for example the situation in our country prior to the swearing in of the 116th Congress: Republicans controlled the Executive and Legislative branches of our government but were unable to approve a budget, leading to a partial government shutdown. Jordain Carney, *Lawmakers Punt Shutdown to New Congress*, HILL (Dec. 31, 2018, 10:36 AM), https://thehill.com/homenews/senate/423314-lawmakers-punt-shutdown-to-new-congress [https://perma.cc/KA6L-GKST].

151. *Automated License Plate Readers: State Legislation 2016 & 2017*, NAT'L CONF. ST. LEGISLATURES (Jan. 2, 2018), https://web.archive.org/web/20180224190105/http://www.ncsl.org/research/telecommunications-and-information-technology/automated-license-plate-readers-state-legislation-2016.aspx [https://perma.cc/5M7J-98D5]. Similarly, in 2016, at least eighteen states considered enacting automated license plate reader bills, but only three states—New Hampshire, Oklahoma, and Vermont—successfully enacted legislation. *Id.* As of March 15, 2019, only sixteen states had enacted statutes regulating the use of automated license plate readers or the retention of automated license plate reader data. *Automated License Plate Readers: State Statutes*, NAT'L CONF. ST. LEGISLATURES (Mar. 15, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/9 4W9-64WN].

152. Farivar, *Your Car, Tracked*, *supra* note 10, at 3.

age of criminal justice reform,[153] there is not yet enough public outcry regarding automated license plate readers for legislators to be properly motivated to take up the issue. Therefore, it is up to the Supreme Court to protect individuals' privacy interests now.

E. Why the Fourth Amendment Should Regulate Not Only the Collection of Information, but Also Its Use

Normally, surveillance involves several stages: acquisition, analysis, and use or disclosure of information.[154] Traditionally, the Fourth Amendment has regulated only the acquisition or collection of information and not its analysis or use.[155] The second two steps have been deemed outside the scope of the Amendment.[156] However, the use of information, and not just the collection of it, should be subject to Fourth Amendment protections and require a search warrant.[157] First, the privacy concerns associated with the government's broad collection power "might not be so alarming if there were reliable limits on how the government used the information in its

153. A George Mason University study found that Virginia residents had complex reactions regarding the use of automated license plate readers:

> [M]ost citizens supported their local police using LPR to check to see if passing vehicles were stolen or to monitor high-risk targets of terrorism . . . . However, ... the majority of respondents considered the data collected by LPR systems to be private, and that policies and protections should be in place for the use of this data.

Id. at 2.

154. Kerr, *supra* note 127, at 331.

155. *Id.*

156. *Id.* at 331–32.

157. Though extending the Fourth Amendment to regulate the use of information and not just its collection is a departure from the Court's current understanding of the Fourth Amendment, it would properly reflect our evolving technology. The Framers of the Constitution could not have imagined the volume of personal information that can be stored on individuals' personal lives and similarly could not have understood how the collection of information might not be as invasive as its aggregation and use. The Framers' lack of foresight should not doom individuals to invasions of their privacy because, at the time, only the acquisition of items posed a threat.

What is more, several commenters have similarly argued for Fourth Amendment regulation of the use of information. *See, e.g.*, Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579–80 (2017) ("The privacy impact of large amounts of data, however, does not come solely from the sweeping nature of the government's *collection* authority. The government's postcollection *use* of information can—and often does—implicate privacy interests just as strongly. . . . The Fourth Amendment should regulate information *use* as well as its *collection* . . . ."); Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1302 (2011) ("If I am right that pervasive surveillance will become the norm, then the problem for constitutional criminal procedure must necessarily shift from the regulation of the state's acquisition of information to the regulation of the state's use and dissemination of that information."). Covey argues that regulating the use of information under the Fourth Amendment is not as radical as some believe, as the exclusionary rule "designedly addresses the legitimate and illegitimate uses of evidence and information in the state's possession." *Id.*

possession."[158] Second, modifying the collection rules would either fail to address concerns which arise only when the information is used and not merely by its collection,[159] such as inferences which can be gleaned from the information's aggregation, or substantially hinder law enforcement.

Further, under the Fourth Amendment, police officers must "particularly describ[e] the place to be searched, and the persons or things to be seized."[160] This particularity requirement is meant to ensure any search conducted is as narrow as possible[161] and poses problems when applied to the acquisition of license plate information by automatic license plate readers. Courts are unlikely to provide search warrants for unfocused, long-term surveillance where police only *anticipate* that someone will commit a crime at some future time and that the license plate information will prove valuable in catching and prosecuting that individual.[162] The unfocused collection of license plate data does not meet the particularity requirement of the Fourth Amendment. A database query would, however. Police could specify the exact license plate to be entered, the database to be queried, and what they hope to find in the database.

CONCLUSION

Automated license plate readers might initially appear not to pose a great threat to privacy interests, but upon closer examination, it becomes evident that, in the aggregate, the pings associated with one license plate can reveal intimate details about an individual's life as a whole. Practical limitations on surveillance once provided individuals with a sense of anonymity. The current situation, however, is different; due to new surveillance technologies, we are no longer anonymous individuals in a crowd. Automated license plate data, when compiled over the span of years, strips us of our anonymity and exposes our lives to police scrutiny. A single query of the data collected by automated license plate readers has the capacity to reveal our familial, political, professional, religious, and sexual associations by revealing those places we most like to visit in one fell swoop.

In *Carpenter v. United States*, the Supreme Court determined that individuals have a right to privacy in the whole of their movements. Given the parallels between cell-site location information, which when acquired by the government in *Carpenter* constituted a search under the Fourth

158. Berman, *supra* note 157, at 603.
159. *See id.* at 580.
160. U.S. CONST. amend. IV.
161. Kerr, *supra* note 127, at 339.
162. *See* Levinson-Waldman, *supra* note 133, at 582.

Amendment, and automated license plate reader data, the latter should be similarly safeguarded. These safeguards should include requiring a search warrant to query a database for information regarding a specific license plate. This requirement ensures that police can collect this highly valuable information while accounting for its highly sensitive nature. At its core, the search warrant requirement is a delicate balancing act, carefully considered and designed to protect both individuals' privacy and the government's interest in security. Requiring a search warrant to query automated license plate reader data prevents needless violations of individuals' privacy and permits police to use the new technology to catch criminals.

Stephanie Foster[*]

* J.D. (2020), Washington University School of Law; B.A. (2016), Washington & Lee University. Thank you to Professor Neil Richards for introducing me to this fascinating topic, and to all the editors at the *Washington University Law Review* for their painstaking work in preparing this piece for publication.