ENHANCING LAW ENFORCEMENT OR COMPROMISING PRIVACY? THE PROBLEM WITH SOUTH CAROLINA'S USE OF AUTOMATIC LICENSE PLATE READERS

William K. Rees*

I. INTRODUCTION

The Fourth Amendment emerged as a direct response to the loathed "'general warrants' and 'writs of assistance'" that plagued policing in the colonial era.[1] These instruments granted British officers unchecked power to invade homes, rummaging for evidence of criminal activity.[2] When the Fourth Amendment was written and ratified, the primary investigative tool envisioned by the framers was the "constable's eyes" aided by a simple

* First and foremost, I express my sincere gratitude to Professor Leventis for her invaluable guidance throughout the writing process. This Note owes its existence to her mentorship and expertise. I am also thankful for the dedicated members of the *South Carolina Law Review,* whose collaboration and feedback were instrumental in refining this Note for publication. Lastly, I would like to thank my friends and family for their unwavering love and encouragement throughout the writing journey. Their support has been a constant source of strength and inspiration.

1. Carpenter v. United States, 585 U.S. 296, 303 (2018).
2. *Id.*

lantern.[3] In contrast, modern searches leverage sophisticated surveillance techniques and technologies that were inconceivable in 1791.[4] One such advanced technology widely used today is Automatic License Plate Readers (ALPRs).[5]

Since 1998,[6] law enforcement agencies nationwide have integrated ALPRs into their operational arsenals,[7] resulting in the extensive deployment of tens of thousands of readers across the country.[8] ALPRs come in two primary configurations: stationary, like those affixed to traffic lights, telephone poles, or highway overpasses; and mobile, such as those mounted on law enforcement vehicles.[9] ALPR systems work by employing a combination of cameras and optical character recognition software to systemically scan the license plates of all passing vehicles—recording details such as the scan's date and time, the vehicle's GPS coordinates, the vehicle's make and model, the speed at which a vehicle is traveling—and take photographs of the vehicle.[10] Some of the photographs even capture the occupants of the vehicle.[11] These readers are able to scan thousands of plates per minute.[12] To put the capabilities of ALPRs in perspective, one vendor proudly asserts that its ALPRs can capture readable plates and detailed vehicle images in "bright daylight and pitchblack darkness."[13] Additionally, the

3. RONALD J. ALLEN ET AT., CRIMINAL PROCEDURE: INVESTIGATION AND RIGHTS TO COUNSEL 379 (4th ed. 2020).

4. *Id.*

5. Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology*, U.S. DEP'T JUST.: BUREAU OF JUST. STAT. (July, 2015), https://bjs.ojp.gov/content/pub/pdf/lpd13et.pdf [https://perma.cc/35WX-QU6Q] (93% of police departments in cities with populations of one million or more used their own ALPR systems in 2013).

6. Lauren Fash, *Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy*, 78 MD. L. REV. 63, 64 (2019) (discussing how ALPR devices originated in the United Kingdom as a way to defend against attacks by the Irish Republican Army and then made its way to North America in 1998).

7. *Id.*

8. Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations [https://perma.cc/Y6GJ-BMG3].

9. *Id.; Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND, https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/XH6Y-YYZZ] [hereinafter *Street-Level Surveillance*].

10. *Id.*

11. *Id.*

12. *Id.*

13. MOTOROLA SOLUTIONS, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/l5m-mobile-lpr-solution.html [https://perma.cc/HME6-KPL5].

vendor maintains that its ALPRs can reliably record license plates on vehicles traveling at speeds of up to 150 miles per hour.[14]

The data law enforcement agencies collect using ALPRs is subsequently uploaded to databases; ensuring seamless accessibility for law enforcement agencies.[15] The retention period of ALPR data fluctuates across agencies, ranging from mere days to several years, with some agencies opting for indefinite retention.[16] The agencies' data is also automatically cross-referenced with a "hot list," which is a catalogued list of license plates that law enforcement is actively seeking.[17] If an ALPR detects a license plate appearing on the hot list, the system immediately notifies the police.[18] Typically, these hot lists contain the license plates of stolen vehicles and vehicles associated with AMBER Alerts for abducted children.[19] However, some hot lists may include vehicles linked to low-level misdemeanors and traffic offenses, such as unpaid parking tickets.[20]

Moreover, law enforcement's utilization of ALPR data often extends beyond the scans acquired through their own devices.[21] Many departments have agreements that provide them with access to private databases housing scans from private ALPRs, as well as those collected by other local and federal law enforcement agencies.[22] For example, Vigilant Solutions, a prominent ALPR vendor owned by Motorola Solutions, offers access to its database containing over five billion license plate scans gathered nationwide.[23] Furthermore, access to ALPR databases is not limited to law enforcement agencies.[24] Businesses frequently employ ALPR location data during the evaluation of loan applications to corroborate that applicant's stated residential address or to identify commercial vehicle usage while investigating insurance claims.[25] Additionally, private neighborhood associations may acquire ALPR systems for neighborhood security purposes.[26] These private entities then have the discretion to decide whether to share any collected data with law enforcement.[27]

14. *Id.*
15. *Street-Level Surveillance*, *supra* note 9.
16. *Id.*
17. *Id.*; Díaz & Levinson-Waldman, *supra* note 8.
18. *Street-Level Surveillance*, *supra* note 9.
19. Díaz & Levinson-Waldman, *supra* note 8.
20. *Street-Level Surveillance*, *supra* note 9.
21. Díaz & Levinson-Waldman, *supra* note 8.
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*

The value ALPRs provide to law enforcement is undeniable.[28] These systems offer a robust tool for enhancing public safety and preventing crime.[29] Law enforcement agencies depend on ALPRs for a myriad of tasks, including verifying a vehicle's presence at a crime scene, monitoring travel patterns, and identifying potentially associated vehicles.[30] This technology has been instrumental in solving numerous crimes, ranging from burglaries and the recovery of stolen vehicles to kidnappings and murders.[31] Government agencies can even find valuable applications for ALPRs outside of law enforcement, such as aiding in traffic management and environmental pollution control.[32] However, the advantages offered by ALPRs come at a price—namely, the erosion of individual privacy.[33]

This Note surveys the relevant Fourth Amendment jurisprudence, offering an analysis of the privacy concerns arising from the unregulated use of ALPRs. In emphasizing the particular susceptibility of South Carolina's ALPR practices to Fourth Amendment challenges, this Note aims to establish guiding principles for courts and legislators to follow in creating laws to regulate ALPR use. Recognizing that the enactment of law is always an exercise in compromise, these principles are intended to strike a balance between the preservation of individual privacy and the unimpeded functionality of law enforcement, that is consistent with the core tenets of the Fourth Amendment. The Note's overarching objective is to provide a comprehensive framework in which to approach the regulation of ALPR technology. Accordingly, this Note explores a range of approaches for regulating the technology and addresses potential drawbacks associated with each approach.

28. *See* Dimitar Kostadinov, *Privacy Implications of Automatic License Plate Recognition Technology*, INFOSEC (Feb. 7, 2014), https://resources.infosecinstitute.com/topics/general-security/privacy-implications-automatic-license-plate-recognition-technology/#gref [https://perma.cc/8QWY-FBDS].

29. *See id.*

30. *Street-Level Surveillance*, *supra* note 9.

31. Randy L. Dryer & S. Shane Stroud, *Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action*, 55 JURIMETRICS J. 225, 226 (2015).

32. Díaz & Levinson-Waldman, *supra* note 8.

33. *See* Kostadinov, *supra* note 28; *Street-Level Surveillance*, *supra* note 9; Díaz & Levinson-Waldman, *supra* note 8.

II. BACKGROUND

A. The Fourth Amendment: A Historical Analysis

The Fourth Amendment of the United States Constitution protects the people against "unreasonable searches and seizures."[34] It endeavors to achieve this protection by "secur[ing] the 'privacies of life' against 'arbitrary power'" and "plac[ing] obstacles in the way of a too permeating police surveillance."[35] Thus, the Fourth Amendment assumes a dual role within the American legal framework, functioning as the chief source of both privacy protection and regulation of law enforcement.[36] These two roles—protecting privacy and regulating the police—require the Fourth Amendment to strike a delicate balance between adequately preserving individual privacy and empowering the police to ensure public safety.[37] In the twenty-first century, as advancements in information technology increasingly jeopardize individuals' privacy, the Fourth Amendment's balancing of these competing interests may be more critical than ever before. As noted by Justice Douglas, "[e]lectronic surveillance is the greatest leveler of human privacy ever known."[38]

Although the Fourth Amendment commences with "[t]he right of the people," the Court's early interpretation limited the amendment's protection to specific locations, such as one's home or its immediate surroundings, referred to as "curtilage."[39] *Olmstead v. United States* illustrates the Court's property-focused interpretation of the Fourth Amendment.[40] In *Olmstead*, federal officers conducted wiretaps on the telephone lines of four residences and one office without obtaining a search warrant, resulting in the interception of incriminating messages that led to the defendants' arrests.[41] Importantly, the wiretapping had been effectuated without a physical trespass by the government.[42] According to the Court's rationale, the absence of a physical trespass meant that the actions did not constitute a Fourth Amendment search.[43] The Court's reasoning was rooted in the belief that the Amendment itself implies a search of "material things"—namely, "the person, the house, his papers, or his effects."[44] Thus, the officers' actions did not violate the

34. U.S. CONST. amend. IV.
35. Carpenter v. United States, 585 U.S. 296, 305 (2018).
36. Allen, *supra* note 3, at 316.
37. *Id.*
38. United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting).
39. *See* Olmstead v. United States, 277 U.S. 438 (1928).
40. *See id.*
41. *Id.* at 456–57.
42. *Id.* at 457.
43. *Id.* at 464.
44. *Id.*

Fourth Amendment because there was no physical intrusion into the defendants' property, only "voluntary conversations secretly overheard."[45] As a result, subsequent case law centered around constitutionally protected areas rather than individual rights; thereby, maintaining the *Olmstead* property rights approach as the Fourth Amendment standard for thirty-nine years.[46]

In *Katz v. United States*, the Court made a significant departure from the property rights approach established in *Olmstead*.[47] Specifically, the Court abandoned the previously held belief that Fourth Amendment protections hinged solely on physical trespass, opting instead for an inquiry centered around an individual's reasonable expectation of privacy.[48] In *Katz*, FBI agents affixed an electronic listening device to the exterior of a telephone booth.[49] The government, aligned with previous precedent, asserted that no search had taken place since there was no physical intrusion into a constitutionally protected area.[50] Nevertheless, the Court rebuffed this contention, emphatically stating that the Fourth Amendment "protects people, not places."[51] According to the Court, what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[52] Thus, the Court ruled that a search had occurred because the defendant entered the telephone booth with the intention of keeping out "uninvited ears."[53] The key consideration after *Katz* became whether the defendant's reasonable expectation of privacy had been violated.[54] Interestingly, the relevant inquiry was articulated in Justice Harlan's concurring opinion, which delineated a two-pronged test for evaluating the

45. *Id.*

46. *See* Commonwealth v. Chaitt, 380 Pa. 532 (1955); People v. Ross, 236 Cal. App. 2d 364 (1965); United States v. Borgese, 235 F. Supp. 286 (1964).

47. *See* 389 U.S. 347 (1967).

48. *Id.* at 353 ("We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

49. *Id.* at 348.

50. *Id.* at 352 ("The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls.").

51. *Id.* at 351.

52. *Id.*

53. *Id.* ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").

54. *See* Florida v. Jardines, 569 U.S. 1 (2013); Kyllo v. United States, 533 U.S. 27 (2001); Florida v. Riley, 488 U.S. 445 (1989); Oliver v. United States, 466 U.S. 170 (1984); Smith v. Maryland, 442 U.S. 735 (1979).

breach of an individual's reasonable expectation of privacy.[55] According to Justice Harlan, one must have "exhibited an actual (subjective) expectation of privacy," and that expectation must "be one that society is prepared to recognize as reasonable."[56]

Katz, while seemingly expanding the scope of Fourth Amendment protection by eliminating the need for a physical intrusion, simultaneously introduced the "knowing exposure" principle—noting that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[57] Using this principle, the Court, in subsequent cases, validated various police surveillance methods and technologies.[58] For example, in *United States v. Knotts*, the Court pronounced that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[59] The case revolved around the police's use of a beeper placed within a container of chloroform to track it to the defendant's secluded cabin, wherein they discovered a drug laboratory for amphetamine production.[60] The Court's rationale rested on the notion that the defendant's location was "voluntarily conveyed to anyone who wanted to look."[61] Moreover, the Court noted that "[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 . . . ."[62] Hence, the Court reasoned that beepers merely facilitated the observation of what was already in plain sight.[63] While the Court declined to "equate[] police efficiency with unconstitutionality,"[64] it left open the question of more long-term surveillance, cautioning that if such widespread practices materialized,

55. *See Katz*, 389 U.S. at 360–61 (Harlan, J., Concurring).

56. *Id.*

57. *Id.* at 351.

58. *See Riley,* 488 U.S. 445; United States v. Knotts, 460 U.S. 276 (1983); *Smith*, 442 U.S. 735.

59. 460 U.S. 276, 281 (1983).

60. *Id.* at 278–79.

61. *Id.* at 281–82 ("When Petschen travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.").

62. *Id.* at 282.

63. *Id.* at 284 ("As noted above, a principal rationale for allowing warrantless tracking of beepers, particularly beepers in or on an auto, is that beepers are merely a more effective means of observing what is already public.") (internal quotation marks and citation omitted).

64. *Id.* ("Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now.").

the suitability of different constitutional principles might need to be examined.[65]

Although *Katz* ostensibly rejected the property rights approach to the Fourth Amendment,[66] this line of reasoning experienced a revival in *United States v. Jones*.[67] In *Jones*, law enforcement monitored the defendant's movements for twenty-eight days through a GPS device discreetly affixed to his vehicle.[68] The government argued that this surveillance did not constitute a search because the defendant had no reasonable expectation of privacy regarding the locations of his vehicle on public roads, which were voluntarily conveyed to all.[69] However, the Court arrived at a different conclusion, asserting that the act of attaching such a device to someone's vehicle and employing it to track their public movements amounted to a search.[70] The basis of this determination was that the government had physically encroached upon private property with the intention of gathering information.[71] In reaching this conclusion, the Court emphasized the importance of safeguarding a level of privacy from government intrusion that aligns with the principles present at the time of the Fourth Amendment's inception.[72] Moreover, the Court noted that *Katz* established that "'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property.'"[73] Accordingly, the Court reasoned that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common law trespassory test."[74] Thus, the Court abstained from addressing the

65. *Id.* at 283–84 ("[I]f 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.").

66. Katz v. United States, 389 U.S. 347, 353 (1967). ("We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

67. *See* United States v. Jones, 565 U.S. 400 (2012).

68. *Id.* at 403.

69. *Id.* at 406 ("The Government contends that the Harlan standard shows that no search occurred here, since Jones has no 'reasonable expectation of privacy' in the . . . locations of the Jeep on the public roads, which were visible to all.").

70. *Id.* at 404.

71. *Id.* at 404–05 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

72. *Id.* at 406 ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'") (citing Kyllo v. United States 533 U.S. 27, 34 (2001)).

73. *Id.* at 407 (citing Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992)).

74. *Id.* at 409.

government's knowing exposure contentions, finding that the defendant's Fourth Amendment rights did not fall within the *Katz* formulation.[75]

While *Jones* was ultimately decided on trespass grounds,[76] two concurring opinions revealed a significant division in the Court's reasoning. In her concurring opinion, Justice Sotomayor agreed with the majority that reaffirmation of the *Olmstead* property rights approach to the Fourth Amendment was sufficient to decide *Jones*.[77] Nevertheless, she wrote separately to articulate her concerns regarding the broader societal implications of modern police surveillance practices.[78] According to Justice Sotomayor, GPS monitoring violates the Fourth Amendment because it "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."[79] Moreover, the records can be stored and effectively "mined" for years, and the inexpensiveness of GPS monitoring compared to conventional surveillance techniques "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[80] Justice Sotomayor's overarching concern was that extensive surveillance fosters an environment akin to a police state, as "[a]wareness that the Government may be watching chills associational and expressive freedoms" and "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[81] Thus, Justice Sotomayor was skeptical that the average individual would reasonably expect their movements to be recorded and aggregated in manner that enables the government to ascertain such sensitive and personal

75. *Id.* at 406 ("But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

76. *Id.* at 404–05.

77. *Id.* at 414 (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.").

78. *See id.* at 414–15 ("Nonetheless, as Justice ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But '[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.' As Justice ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations.") (internal citations omitted).

79. *Id.* at 415.

80. *Id.* at 415–16.

81. *Id.* at 416 (citing United States v. Cuevas-Perez, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

information.[82] Even so, Justice Sotomayor was content to reserve such a judgment for a case in which the facts could not substantiate a physical trespass.

In contrast, Justice Alito, joined by three other Justices, assumed a more proactive stance, accusing the Court of deciding the case "based on 18th-century tort law."[83] He denounced the majority's trespass approach as "unwise" and "artificial," advocating instead for the need to analyze the use of the GPS tracking device under the *Katz* reasonable expectation of privacy test.[84] In support of his position, Justice Alito noted that individuals in the "pre-computer age" 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. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[85]

Accordingly, he concluded that protracted GPS monitoring violates the Fourth Amendment, as individuals did not anticipate that law enforcement would surreptitiously track and record their every movement over an extended period of time.[86] Justice Alito reached this conclusion despite the fact that the Court earlier determined in *Knotts* that a person traveling in a car on public thoroughfares has no reasonable expectation of privacy in their movements from one place to another.[87] Even so, he contended that relatively brief monitoring of an individual's movements aligns with the privacy expectations

82. *Id.* ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

83. *Id.* at 418 (Alito, J., concurring).

84. *Id.* at 419 (Alito, J., concurring).

85. *Id.* at 429.

86. *Id.* at 430–31 ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's care for a very long period. . . . For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.").

87. *C.f.* United States v. Knotts, 460 U.S. 276 (1983).

that society has acknowledged as reasonable.[88] Despite distinguishing between short- and long-term surveillance,[89] Justice Alito refrained from pinpointing the precise juncture at which tracking a vehicle on public streets constitutes a search.[90] He did, however, state that "the line was surely crossed before the 4-week mark."[91]

Although the decision to reverse in *Jones* was unanimous, the variance in the Justices' reasoning creates uncertainty regarding which legal framework law enforcement should follow when using GPS to track a suspect's public movements. On the one hand, the majority opinion suggests that the use of GPS tracking without a physical intrusion on the suspect's property is permissible under the Fourth Amendment. On the other hand, the concurrences indicate that GPS tracking may violate the Fourth Amendment even in the absence of a physical intrusion, as five Justices agreed that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[92] Fortunately, *Carpenter v. United States* helped clarify this issue by solidifying what a majority of the *Jones* Court already recognized— "that individuals have a reasonable expectation of privacy in the whole of their physical movements."[93]

In *Carpenter*, law enforcement obtained access to 127 days' worth of cell-site location information (CSLI) through a court order.[94] Ultimately, the Court determined that the acquisition of this information constituted a search within the meaning of the Fourth Amendment.[95] This conclusion arose from a re-examination of the fundamental tenets of the Fourth Amendment, coupled with a careful review of past precedents in the context of evolving technology.[96] Through this historical analysis, the Court found that this sort of digital data did "not fit neatly under existing precedents"[97] because it was

88. *Jones,* 565 U.S. at 430 ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

89. *Id.*

90. *Id.* ("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.").

91. *Id.*

92. *Id.; Id.* at 415 (Sotomayor, J., concurring).

93. 585 U.S. 296, 310 (2018).

94. *Id.* at 309.

95. *Id.* at 316.

96. *See id.* at 305.

97. *Id.* at 306 ("This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.").

"far more intrusive than the precedents might have anticipated."[98] Notably, the Court declined to apply the principle set forth in *Knotts*, which posited that individuals have no reasonable expectation of privacy in their public movements.[99] The Court pointed out that *Knotts* "was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance."[100] In light of this distinction, the Court declared that individuals do not "surrender all Fourth Amendment protection by venturing into the public sphere."[101] Instead, the Court, citing Justice Alito's and Justice Sotomayor's concurring opinions in *Jones*, reasoned that "[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[102] That the movements occurred in public did not negate the entitlement to protection against overly pervasive police surveillance.[103]

The Court also rejected an argument based on the third-party doctrine.[104] The third-party doctrine, which stems from the *Katz* "knowing exposure" principle, holds that individuals who voluntarily share information with third parties relinquish any reasonable expectation of privacy in that information.[105] The government's primary contention was that the CSLI was fair game because they were business records created and maintained by the wireless carriers.[106] However, according to the Court, the collection of CSLI did not align with the voluntary exposure rationale underpinning the third-party doctrine.[107] As the Court observed, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation."[108] Furthermore, the Court noted that the cell-site location information is collected "without any affirmative act on the part of the user beyond powering up."[109] Thus, the Court reasoned that the user does not "voluntarily 'assume[ ] the risk' of turning over a comprehensive

98. *Smart Cities: Fourth Amendment*, CENTER FOR LEGAL & COURT TECHNOLOGY, https://law.wm.edu/academics/intellectuallife/researchcenters/clct/exhibit-ai/additional-resources/exhibit-ai---exhibit-8---additional-resources.pdf [https://perma.cc/NCV7-AAL6].

99. *See Carpenter*, 585 U.S. at 306.

100. *Id.*

101. *Id.* at 310.

102. *Id.*

103. *Id.*

104. *Id.* at 309 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

105. *Id.* at 308 ("We have previously held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'") (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

106. *Id.* at 313.

107. *Id.* at 315.

108. *Id.* (internal citation omitted).

109. *Id.*

dossier of his physical movements," as "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[110] Accordingly, the Court declined to extend the third-party doctrine to the collection of cell-site location information.[111]

The Court found several key aspects of CSLI particularly troubling, echoing the concerns expressed by Justice Alito and Justice Sotomayor in their *Jones* concurrences. For one, the Court highlighted the absence of practical constraints, such as limited funding, that had previously curbed the government's access to such a "deep repository of historical location information."[112] As the Court observed, CSLI offered a comprehensive record of individuals' movements, opening "an intimate window into a person's life."[113] In the Court's assessment, this level of detail revealed not only specific movements but also private aspects of a person's existence, including their "'familial, political, professional, religious, and sexual associations.'"[114] The Court also expressed apprehension about the retrospective nature of the records, which enabled the government to "travel back in time to retrace a person's whereabouts" and granted access "to a category of information otherwise unknowable."[115] Furthermore, the collection of CSLI was not confined only to those suspected of criminal wrongdoing.[116] The Court distinguished the case from *Jones* where the police needed to identify the target before tracking them.[117] With cell-site location information, the government could chronicle the past movements of anyone, irrespective of suspicion of criminal activity.[118] As the Court put it, "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."[119]

Despite the Court's attempt in *Carpenter* to bring the law in conformity "with the seismic shifts in digital technology,"[120] it maintained that its ruling

110. *Id.* (internal citation omitted).

111. *Id.* ("We therefore decline to extend *Smith* and *Miller* to the collection of CSLI.").

112. *Id.* at 311 ("And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.").

113. *Id.* at 311.

114. *Id.* (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

115. *Id.* at 312.

116. *See id.* ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

117. *Id.* ("Unlike with the GPS device in *Jones,* police need not even know in advance whether they want to follow a particular individual or when.").

118. *Id.*

119. *Id.*

120. *Id.* at 313.

was "a narrow one."[121] Specifically, the Court aimed to restrict its judgment solely to cell-site location information, without "call[ing] into question conventional surveillance techniques and tools, such as security cameras."[122] The Court's purpose in cabining its opinion was to avoid "embarrass[ing] the future."[123] However, by presuming that security cameras are exempt from the concerns it addressed, the Court may have actually invited future complications rather than prevented them. After all, automatic license plate readers are simply security cameras adapted to a different use, blurring the lines between what the Court considers conventional and contemporary surveillance tools.

B. How Courts Have Applied Carpenter

1. Federal Courts

Although *Carpenter* seemingly exempted security cameras from privacy concerns, the Fourth Circuit challenged this presumption in *Leaders of Beautiful Struggle v. Baltimore Police Department*.[124] That case revolved around the Baltimore Police Department's Aerial Investigation Research (AIR) program, which utilized planes equipped with cameras to surveil Baltimore City.[125] The significance of *Carpenter*, as the Fourth Circuit saw it, was that it "solidified the line between short-term tracking of public movements . . . and prolonged tracking that can reveal intimate details through habits and patterns."[126] Contrary to the district court's view, the Fourth Circuit found that the AIR program fell into the latter category of surveillance, infringing upon individuals' reasonable expectation of privacy in the whole of their movements.[127] In reaching this conclusion, the court engaged in a direct comparison of the AIR program data to the cell-site location information in *Carpenter*, unveiling numerous similarities.[128] The court noted that the AIR program's forty-five-day retention policy created a detailed

121. *Id.* at 316.

122. *Id.*

123. *Id.* ("[T]he Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'") (citing Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

124. *See* 2 F.4th 330, 333 (2021).

125. *Id.* at 333.

126. *Id.* at 341.

127. *Id.* at 342 ("The latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant. . . . "That the Defendants chose to limit the data collection to daylight hours and a certain resolution does not make the AIR program equivalent to traditional, short-term surveillance.").

128. *See id* at 341–45.

record of individuals' movements over the preceding month and a half.[129] Thus, the AIR program data, like cell-site location information, allowed retrospective location tracking of everyone, not just those suspected of criminal wrongdoing.[130]

Interestingly, the district court had refused to analogize the Baltimore Police Department's use of the AIR program to cell-site location information.[131] The basis of the district court's opinion was that the AIR program had restricted tracking capabilities because data collection was confined to daylight hours; the photographic resolution was limited to one pixel per person or vehicle; and the program was inoperable during inclement weather.[132] Thus, the district court reasoned that the AIR program "could not expose the 'privacies of life,'" as the inherent gaps in the data hindered law enforcement's ability to track suspects across multiple days.[133] However, the Fourth Circuit considered the data gaps insignificant, as the information was abundant enough to make deductions about private aspects of individuals' lives—"the epitome of information expected to be beyond the warrantless reach of the government."[134] Moreover, the court observed that the

129. *Id.* at 341 ("Because the data is retained for 45 days—at least—it is a 'detailed, encyclopedic,' record of where everyone came and went within the city during daylight hours over the prior month-and-a-half.") (citing Carpenter v. United States, 138 S.Ct. 2206, 2218 (2018).

130. *Id.* at 341–42 ("Law enforcement can 'travel back in time' to observe a target's movements, forwards and backwards. Without technology, police can attempt to tail suspects, but AIR data is more like 'attach[ing] an ankle monitor' to every person in the city. 'Whoever the suspect turns out to be,' they have 'effectively been tailed' for the prior six weeks. Thus, the 'retrospective quality of the data' enables police to 'retrace a person's whereabouts,' granting access to other 'unknowable' information.") (citing Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)).

131. *Id.* at 340 ("Plaintiffs argued the AIR program violates *Carpenter*. The district court rejected this analogy, relying on precedents that approved warrantless pole cameras and flyover photography, and distinguishing CSLI as 'a far more intrusive, efficient, and reliable method of tracking a person's whereabouts.'") (internal citation omitted).

132. *Id.* ("The district court's conclusion arose from its read of the facts: 'the AIR program has limited location-tracking abilities' because it 'will only depict individuals as miniscule dots moving about a city landscape'; the planes 'will not fly at night and cannot capture images in inclement weather'; and 'gaps in the data will prohibit that tracking of individuals over the course of multiple days.'") (internal citation omitted).

133. *Id.* ("From that premise, it believed that the AIR program could not expose the 'privacies of life.'") (internal citation omitted).

134. *Id.* at 342 ("We do not suggest that the AIR program allows perfect tracking of all individuals it captures across all the time it covers. Though the data is collected in 12-hour increments, the tracks are often shorter snippets of several hours or less. Still, the program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips. It enables deductions about 'what a person does repeatedly, what he does not do, and what he does ensemble,' which

government's ability to deduce intimate information about individuals' lives was heightened by the government's capacity to cross-reference the AIR program data with data from other surveillance systems.[135] Notably, the court explicitly mentioned license plate readers as one of the data systems the police could use in conjunction with the AIR program data,[136] suggesting its view that license plate readers constituted a permissible form of surveillance when used alone. Even so, the Fourth Circuit's ruling in *Leaders of a Beautiful Struggle* illuminates a critical point: traditional surveillance tools, when repurposed for innovative applications, may encroach upon individuals' reasonable expectations of privacy.

2. State Courts

While the Fourth Circuit has yet to address the constitutional implications of ALPRs, state courts have been more receptive to these concerns.[137] For example, in *Commonwealth v. McCarthy*, the Supreme Judicial Court of Massachusetts found that widespread ALPR use could implicate constitutional protections against unreasonable searches.[138] In *McCarthy*, law enforcement utilized four ALPR cameras positioned at two fixed locations on opposite ends of two bridges to surveil the defendant's movements over a three-month period.[139] The defendant contested the warrantless search of the ALPR data;[140] however, the court held that the limited use of ALPRs in this case did not constitute a search under the Fourth Amendment.[141] Consequently, the court affirmed the denial of the defendant's motion to suppress.[142] While the court refrained from specifying the threshold at which

"reveal[s] more about a person than does any individual trip in isolation.'") (internal citations omitted).

135. *Id.* at 344 ("Further, the AIR program does not deduce identity from randomly selected location points, like in a research study. Rather, the context of a specific investigation narrows the pool of possible identities. Police can cross-reference against publicly available information and, even more valuably, their own data systems.").

136. *Id.* ("PSS can enhance the process by integrating BPD systems—like its CitiWatch camera network, license plate readers, and gunshot detectors—into its 'iView software,' 'mak[ing] all the systems work together.") (internal citation omitted).

137. *See, e.g.*, Commonwealth v. McCarthy, 142 N.E.3d 1090 (2020).

138. *Id.* at 1095.

139. *Id.*

140. *Id.* at 1097 ("Defendant filed motions to suppress the ALPR data and the fruits of the arrest.").

141. *Id.* at 1095 ("We conclude that, while the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest is not invaded by the limited extent and use of ALPR data in this case.").

142. *Id.* at 1109.

ALPR usage invokes constitutional protections,[143] it made clear that it would reach a different conclusion in cases involving more pervasive ALPR systems.[144] Specifically, the court reasoned that "[w]ith enough cameras in enough locations, the historic location data from an ALPR system . . . would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes."[145] This dicta in *McCarthy* indicates that ALPR use may merit greater constitutional scrutiny in future cases.[146]

C. Relationship Between the Federal and South Carolina Constitutions

The prospect of ALPRs facing greater constitutional scrutiny seems more likely in states like South Carolina, which provide heightened privacy protections beyond those mandated by the Fourth Amendment.[147] The Fourth Amendment's prohibition against "unreasonable searches and seizures" safeguards the rights of every citizen in all criminal proceedings.[148] The South Carolina constitution operates in tandem with the Fourth Amendment, providing supplementary safeguards against unauthorized searches and seizures.[149] State legislatures have the authority to grant broader rights under state constitutional provisions than those guaranteed by the federal Constitution.[150] This dynamic is commonly characterized "as a recognition that the federal Constitution sets the floor for individual rights while the state constitution establishes the ceiling."[151] Thus, South Carolina state courts can

143. *Id.* at 1106. ("While we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections, it is not that produced by four cameras at fixed locations on the ends of two bridges.").

144. *Id.* at 1104.

145. *Id.*

146. *See id.* at 1104, 1109 ("For while no ALPR network is likely to be as detailed in its surveillance as GPS or CSLI data, one well may be able to make many of the of the same inferences from ALPR data that implicates expressive and associative rights.") (citing American Civ. Liberties Union Found. Of S. Cal. v. Superior Court of Los Angeles Cnty., 3 Cal. 5th 1032, 1044 (2017)); "While we recognize that the widespread use of ALPRs . . . could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not.").

147. *See* State v. Forrester, 343 S.C. 637, 644, 541 S.E.2d 837, 841 (2001).

148. *Id.* at 643, 541 S.E.2d at 840.

149. *Id.* ("In parallel with the protection of the Fourth Amendment, the South Carolina Constitution also provides a safeguard against unlawful searches and seizures.") (citing S.C. CONST. art. 1 § 10).

150. *Id.* ("The relationship between the two constitutions is significant because '[s]tate courts may afford more expansive rights under state constitutional provisions than the rights which are conferred by the Federal Constitution.") (citing State v. Easler, 327 S.C. 121, 131 n.13, 489 S.E.2d 617, 625 n. 13 (1997)).

151. *Id.* (citing Segura v. Texas, 826 S.W.2d 178, 182 (Tex. App. 1992)).

interpret state law to provide citizens with an additional layer of protection against unlawful searches and seizures.[152]

South Carolina's constitution, in addition to replicating the language of the Fourth Amendment, contains an explicit protection of the right of privacy:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures *and unreasonable invasions of privacy* shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.[153]

According to the Supreme Court of South Carolina, by expressly prohibiting "'unreasonable invasions of privacy,'" the legislature has "indicated that searches and seizures that do not offend the federal constitution may still offend the South Carolina Constitution."[154] Thus, the court reasoned that South Carolina's constitution "favors an interpretation offering a higher level of privacy protection than the Fourth Amendment."[155] Accordingly, law enforcement surveillance technologies that might escape the classification of a search under the Fourth Amendment may nevertheless constitute a search under the South Carolina constitution.

D. South Carolina ALPRs

The South Carolina Law Enforcement Division (SLED) is one of the many law enforcement agencies across the country utilizing a comprehensive statewide network of ALPRs to record and store millions of license plate images annually.[156] These images, termed "reads" by SLED, encompass digital snapshots of license plates and vehicles, complete with vital metadata including date, time, and geographical coordinates.[157] This wealth of information is meticulously organized within SLED's expansive database, aptly named the "Back Office," which acts as a centralized hub, pooling

152. *Id.* at 644, 541 S.E.2d at 840. ("Thus, this Court can interpret the state protection against unreasonable searches and seizures in such a way as to provide greater protection than the federal Constitution.").

153. S.C. CONST. art. 1 § 10 (emphasis added).

154. *Forrester*, 343 S.C. at 644, 541 S.E.2d at 841.

155. *Id.* at 645, 541 S.E.2d at 841.

156. Policing Project, *SCPIF v. SLED,* NYU SCHOOL OF LAW, https://www.policingproject.org/south-carolina-license-plate-reader-lawsuit [https://perma.cc/392A-C48G].

157. *See* Policing Project, *SCPIF v. SLED, Exhibits,* NYU SCHOOL OF LAW, at 10, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/6434d73559e6c8337894dcd7/1681184565793/SCPIF+v.+SLED+-+Exhibits.pdf [https://perma.cc/SPA2-63YT].

ALPR data from forty-eight law enforcement agencies throughout South Carolina.[158] Despite the data contributed to the Back Office being retained for a period of only three years, SLED amassed an astonishing collection of over four hundred million license plate reads by 2022.[159] This trove of data is far from static and it continues to expand at a rapid pace.[160] In 2021 alone, SLED processed a staggering 150 million license plate reads—up from 135 million in 2020 and 26 million in 2014.[161] The database's rapid growth shows no signs of slowing down; propelled by the continuous integration of new ALPR cameras by various municipalities, all seamlessly feeding their data into this colossal repository.[162]

This extensive archive of information is not confined to internal use; it is disseminated to ninety-nine municipal, state, and federal agencies, ensuring broad accessibility.[163] To maintain some semblance of control, SLED's ALPR policy imposes certain criteria on users of the database: only officers possessing National Crime Information Center (NCIC) inquiry certification and authorized credentials, in the form of usernames and passwords provided by SLED, are permitted to access the Back Office.[164] However, despite these ostensibly demanding measures, the active user base currently stands at 2,077,[165] raising questions about the stringency of this standard.

The Back Office is a searchable database, allowing individuals or agencies with authorized access to conduct searches based on a license plate, a partial license plate, or an address.[166] A Back Office search based on a license plate will generate a report of every image of that plate in the database, along with the date, time, and location of each image that was taken.[167] A search based on an address will generate a report of all license plates captured

158. *Id.* at 30.

159. *See* Policing Project, *SCPIF v. SLED, Complaint,* NYU SCHOOL OF LAW, at 9, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/6434d6b649164819cf971985/1681184439055/SCPIF+v.+SLED+-+Complaint+for+Declaratory+and+Injunctive+Relief+%282%29.pdf [https://perma.cc/55FW-AV4S].

160. *See id.* at 4.

161. *Id.* at 9.

162. *See* Rickey Ciapha Dennis Jr.*, North Charleston Planning to Add Over 700 Cameras Around the City to Expand Surveillance,* THE POST AND COURIER (Apr. 28, 2022), https://bit.ly/3FKNdNr [https://perma.cc/Q5YZ-4T5R]; Corinne McGrath*, Horry County Police Department to Install 23 License Plate Readers to Combat Crime*, WMBF (Mar. 21, 2022), https://bit.ly/3t5FaDa [https://perma.cc/HY62-S6B6]; *Simpsonville Uses Automated License Plate Readers to Help Fight Crime*, WSPA (Mar. 31, 2021), http://bit.ly/3T4P3Mg [https://perma.cc/NUP3-69JE].

163. *See* Policing Project, *supra* note 157.

164. *Id.*

165. *Id.*

166. *See* Project Policing, *supra* note 159.

167. *Id.*

at or near a location of the user's choosing.[168] For each search, the user has the flexibility to tailor their results.[169] They can opt for a comprehensive overview spanning the entire three-year dataset, or alternatively, narrow their focus by specifying a precise time frame.[170]

There is no evidentiary threshold an officer must satisfy before conducting a search of the Back Office.[171] The only restriction SLED imposes on law enforcement's use of the Back Office is that it be for a "legitimate law enforcement purpose" or "public safety-related mission."[172] SLED's ALPR policy does not define these terms, inviting subjective and potentially discriminatory interpretations by users searching the database.[173] Adding to the ambiguity, the legislature has failed to provide any specific guidance on SLED's utilization of the ALPR system.[174] The legislature has given SLED the exclusive authority to operate and maintain a statewide criminal justice database,[175] "with such functions as the Division may assign to it."[176] However, unlike other criminal justice databases SLED maintains, such as the DNA database,[177] there is no specific statute governing SLED's use of an ALPR database.[178] As a result, SLED is entrusted with self-regulating its ALPR use.[179]

SLED's ALPR program has already come under fire for its lack of statutory authority.[180] The South Carolina Public Interest Foundation (SCPIF), in collaboration with a Greenville resident, recently filed a lawsuit against SLED concerning its statewide ALPR database.[181] The basis of the lawsuit is that SLED exceeded its statutory authority by unilaterally enacting the ALPR program without any guidance or permission from the legislature.[182] Interestingly, SCPIF declined to challenge the legality of the program under the Fourth Amendment, despite acknowledging that that SLED's ALPR database implicates the privacy rights of millions of South

168. *Id.*
169. *See id.*
170. *Id.*
171. *See* Project Policing, *supra* note 159, at 8.
172. *See* Project Policing, *supra* note 157, at 12.
173. *See id.*
174. Joshua Manson, *South Carolinians Sue to End Unauthorized Police Surveillance*, POLICING PROJECT AT N.Y.U. SCH. OF L. (Apr. 11, 2023), https://www.policingproject.org/scpif-v-sled [https://perma.cc/8JES-VBLV].
175. S.C. Code Ann. § 23-3-15(A)(4) (2003).
176. S.C. Code Ann. § 23-3-110 (1962).
177. S.C. Code. Ann. § 23-3-600 (1994).
178. *Manson*, *supra* note 174.
179. *See id.*
180. *See id.*
181. *Id.*
182. *See* Project Policing, *supra* note 159, at 4.

Carolina residents.[183] Thus, the question remains: does SLED's use of an ALPR database constitute a search under the Fourth Amendment?

III. ANALYSIS UNDER *CARPENTER*

ALPR systems epitomize the concern Justice Alito highlighted in his *Jones* concurrence—the ability to bypass the practical constraints on law enforcement that formerly safeguarded individuals during the "pre-computer age."[184] Prior to the advent of ALPRs, license plate numbers had to be manually recorded, a process that inherently restricted the scope and duration of police surveillance efforts.[185] To track a vehicle for any extended period of time "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance."[186] In contrast, ALPR technology can scan and record license plate numbers at an unprecedented speed and volume without any affirmative effort from police, significantly amplifying law enforcement's data collection capabilities.[187] ALPRs are not only efficient but are also cost effective.[188] Unlike many advanced surveillance technologies, these systems can achieve this heightened surveillance without burdening law enforcement agencies with exorbitant costs.[189] The economical nature of ALPRs facilitates long-term monitoring in a diverse range of investigations, not just those of "unusual importance."[190]

While ALPR technology circumvents the practical constraints that historically protected individual privacy, the crux of the issue is not inherent to the technology itself, but rather stems from the data aggregation it enables. With ALPR information from forty-eight law enforcement agencies across South Carolina feeding into the Back Office,[191] SLED's ALPR database, like the database in *Carpenter*, is "detailed" and "encyclopedic,"[192] "provid[ing] an all-encompassing record of the [driver's] whereabouts."[193] Access to such

183. *Id.* ("The program implicates the privacy interests and individual rights of millions of South Carolina residents whose movements are being recorded and monitored by an unauthorized surveillance database.")

184. United States v. Jones, 565 U.S. 400, 419 (2012) (Alito, J., concurring).

185. *Street-Level Surveillance, supra* note 9.

186. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

187. *Street-Level Surveillance*, *supra* note 9; Díaz & Levinson-Waldman, *supra* note 8.

188. *See* Kostadinov, *supra* note 28.

189. *Id.*

190. *Jones*, 546 U.S. at 429 (Alito, J., concurring) (referring to Justice Alito's remarks that the surveillance at issue in *Jones* "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," which is an expenditure only an "investigation of unusual importance could have justified.").

191. *See* Project Policing, *supra* note 157, at 4.

192. United States v. Carpenter, 585 U.S. 296, 309 (2018).

193. *Id.* at 311.

a "deep repository of historical location information"[194] reveals far more than the public movements of individuals contemplated by the Court in *Knotts.* It opens an "intimate window into a person's life,"[195] empowering law enforcement to pinpoint sensitive places individuals frequent, including their residences, workplaces, healthcare facilities, and places of worship.[196] The stored data even enables law enforcement to make accurate predictions about individuals' future whereabouts.[197]

Moreover, SLED's three-year retention policy[198] gives it the ability to enter a virtual time machine and view an individual's past movements. Before ALPRs, SLED's "attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection."[199] However, with the retrospective nature of the Back Office data, SLED can now do what concerned the Court, "travel back in time to retrace a person's whereabouts," giving it access to "a category of information otherwise unknowable."[200] Further, SLED's ALPR database indiscriminately preserves records of all drivers, regardless of any suspicion of criminal activity. In fact, less than one percent of vehicles scanned nationwide are linked to any criminal activity or wrongdoing.[201] Thus, South Carolina law enforcement "need not even know in advance whether they want to follow a particular individual, or when."[202] Rather, "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for [three] years . . . ."[203]

South Carolina citizens, like all American citizens, have a reasonable expectation of privacy in the whole of their physical movements.[204] The determination of whether South Carolina law enforcement invades this expectation in the way that concerned the Court in *Carpenter*, hinges on the scope of the Back Office search. Justice Alito noted that relatively brief monitoring of an individual's whereabouts, comparable to what law enforcement could achieve without the assistance of modern surveillance technology, does not infringe upon reasonable expectations of privacy.[205] However, as a majority of Justices in *Jones* agreed, prolonged surveillance of public movements by SLED unveils intimate aspects of South Carolina

194. *Id.*
195. *Id.*
196. *Street-Level Surveillance*, *supra* note 9.
197. *Id.*; Díaz & Levinson-Waldman, *supra* note 8.
198. *See* Project Policing, *supra* note 157, at 4.
199. United States v. Carpenter, 585 U.S. 296, 312 (2018).
200. *Id.*
201. *Street-Level Surveillance*, *supra* note 9; Díaz & Levinson-Waldman, *supra* note 8.
202. *Carpenter*, 585 U.S. at 312.
203. *Id.*
204. *See id.* at 310.
205. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (citing United States v. Knotts 460 U.S. 276, 281–82 (1983)).

citizens' lives, thereby constituting a search under the Fourth Amendment.[206] Notwithstanding Justice Alito's observation that "the line was surely crossed before the 4-week mark,"[207] the distinction between short-term and long-term surveillance remains unclear. The absence of a clearly defined line deprives South Carolina law enforcement of the necessary guidance for the lawful utilization of SLED's ALPR database and places the privacy of South Carolina citizens at a perpetual risk of intrusion.

IV. PROPOSED SOLUTION

A. Judicial

To safeguard the rights of South Carolina citizens, a court tasked with adjudicating a challenge to SLED's ALPR database ought to strive for a precise delineation between short- and long-term tracking of an individual's movements. Recognizing the latter as a search within the meaning of the Fourth Amendment, the court should mandate law enforcement agencies to secure a warrant for such surveillance, while exempting short-term tracking from this requirement. Thus, by definitively delineating the threshold between short- and long-term tracking, the court would effectively define the parameters of law enforcement's warrantless utilization of the ALPR database. An informed understanding of the Court's reasoning in *Carpenter*, coupled with the perspectives articulated by Justices Alito and Sotomayor in their *Jones* concurrences, suggests that a warrantless search of the Back Office should be confined to the data associated with an individual trip.

This proposal is rooted in an understanding of the data law enforcement could feasibly acquire without the data aggregation made possible by modern surveillance technologies. For example, if an officer suspects an individual is involved in some form of criminal wrongdoing, it would be reasonable for the officer to tail the suspect in an attempt to ascertain information that could implicate the suspect in the alleged crime. According to Justice Alito, this type of surveillance "accords with expectations of privacy that our society has recognized as reasonable."[208] However, absent extraordinary circumstances justifying a substantial expenditure of law enforcement resources, no individual reasonably anticipates continuous monitoring spanning multiple days, let alone years. Indeed, as Justice Alito observed, such extensive monitoring is virtually impossible without contemporary surveillance technology.[209] By limiting the warrantless utilization of the Back Office to

206. *See id.* at 430–31.
207. *Id.* at 430.
208. *Id*. at 430.
209. *See id.* at 429.

data obtained from individual trips, a South Carolina trial court would align South Carolina law enforcement's tracking capabilities with South Carolina citizens' reasonable expectations of privacy. That is, a warrantless search of the Back Office would not unveil the entirety of an individual's physical movements; instead, it would only disclose an individual's observable whereabouts at a specific moment in time.

Limiting warrantless use of the Back Office in this way would address many of the concerns expressed by the Court in *Carpenter*. For one, law enforcement's tracking capabilities under such a restriction would be akin to those in the "pre-computer age."[210] As a result, the absence of practical constraints on law enforcement's surveillance, such as limited funding, would be rendered inconsequential, as the restriction would curtail law enforcement's access to such a "deep repository of historical location information."[211] Secondly, the insights law enforcement gleans from a warrantless search of the Back Office would be confined to a single trip viewed in isolation, thereby preventing law enforcement from making deductions that intrude on private facets of South Carolina citizens' lives. Furthermore, a one trip restriction would hinder law enforcement's ability to "travel back in time to retrace a person's whereabouts," as warrantless access to data would be limited to an individual trip, irrespective of its temporal proximity to the search.[212]

Moreover, a one trip restriction is particularly well-suited for South Carolina, as it aligns with the Fourth Circuit's understanding of *Carpenter*.[213] In *Leaders of Beautiful Struggle*, the Fourth Circuit found that the intrusive tracking capabilities of Baltimore's Air program invaded reasonable expectations of privacy because its data collection was "enough to yield 'a wealth of detail,' greater than the *sum of individual trips*."[214] Further, the court noted that the program "enable[d] deductions about 'what a person does repeatedly, what he does not do, and what he does ensemble,' which 'reveal[s] more about a person than does *any individual trip viewed in isolation*.'"[215] This reasoning sheds light on the Fourth Circuit's perspective on the distinction between short- and long-term tracking, suggesting that accessing data beyond that derived from an individual trip constitutes long-term tracking. The proposed restriction gains even greater resonance when the

210. *See id.*

211. United States v. Carpenter, 138 S.Ct. 2206, 2218 (2018).

212. *Id*.

213. *See generally* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021).

214. *Id.* at 342 (emphases added) (citing United States v. Jones, 565 U.S. 400, 415–17 (2012) (Sotomayor, J., concurring)).

215. *Id.* (emphases added) (citing United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010)).

Fourth Circuit's rationale is considered in conjunction with the heightened Fourth Amendment protection afforded to South Carolina citizens.[216]

While the proposed restriction effectively addresses many concerns raised by the Court in *Carpenter*, a notable shortcoming arises—it does not adequately tackle the indiscriminate nature of SLED's ALPR data.[217] Accordingly, the adjudicating court should also seek to establish an evidentiary threshold for the warrantless use of the Back Office. Without such a threshold, the proposed restriction may inadvertently permit the misuse of the Back Office by allowing law enforcement access to anyone's location data, provided that it does not exceed data derived from an individual trip.

Fortunately, the court need not embark on a novel endeavor to institute an evidentiary threshold for warrantless use of the Back Office, as Fourth Amendment law already offers a well-suited standard—reasonable suspicion.[218] Under this standard, an officer seeking to justify a warrantless search "must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant the intrusion."[219] Notably less demanding than the probable cause standard required for warrants, the reasonable suspicion standard allows a search "with information that is different in quantity or content" and "can arise from information that is less reliable" than that necessary to demonstrate probable cause.[220] Consequently, reasonable suspicion grants officers the a more constrained authority to conduct a search than probable cause.[221] As such, the reasonable suspicion standard aligns well with the context of warrantless Back Office use, as the modest requirements of this standard proportionately match the limited data associated with an individual trip.

In sum, the solution proposed by this achieves the overarching objective of the Fourth Amendment—preserving individual privacy without unduly hampering law enforcement. Under the proposed solution, SLED is empowered to ensure public safety by retaining the enhanced surveillance capabilities offered by its ALPR database, without a significant drain on resources. Simultaneously, the proposed restriction ensures that SLED's utilization of the database does not infringe upon reasonable expectations of privacy. However, while courts wield considerable authority in devising judicial solutions, their power is constrained by an inherent limitation—they can only rule on issues that are presented to them.[222] Consequently, the

216. *See* State v. Forrester, 343 S.C. 637, 644, 541 S.E.2d 837, 841 (2001).

217. *Carpenter*, 585 U.S. at 312.

218. *See* Terry v. Ohio, 392 U.S. 1, 19 (1968).

219. *Id.* at 21.

220. Alabama v. White, 496 U.S. 325, 330 (1990).

221. *Reasonable Suspicion,* CORNELL L. SCH., https://www.law.cornell.edu/wex/reasonable_suspicion [https://perma.cc/MCJ3-MNS4].

222. *See* Osborn v. Bank of the U.S., 22 U.S. 738, 819 (1824).

proposed restriction can only be implemented by a court if SLED's ALPR database is challenged on Fourth Amendment grounds. Acknowledging this infirmity, the Justice Alito noted that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[223]

B. Legislative

The legislature possesses certain institutional advantages that make it better suited to address the privacy issues raised by new technologies.[224] Namely, legislatures have the ability to act more swiftly than courts due to their broader scope of action, unconstrained by the specific issues brought before them.[225] Indeed, as Justice Alito observed in his *Jones* concurrence, "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[226]

A number of states have heeded Justice Alito's counsel, as at least sixteen state legislatures have enacted statutes that expressly regulate the use of ALPRs.[227] A prominent feature among these statutes are provisions regulating the retention of data collected by ALPRs.[228] The majority of these states limit data retention to a matter of days, while some states have opted for a retention period as brief as a few minutes.[229] South Carolina seeks to follow suit and explicitly regulate the use of ALPRs, as a bill addressing the use of ALPRs is currently under consideration in the House Committee on Judiciary.[230] If passed, this legislation would curtail SLED's ALPR data retention to a period of ninety days.[231] Such a restriction would prevent South Carolina law enforcement agencies from delving into the past and uncovering intimate details of individuals' private lives. Even so, the proposed statute is not adequate.

Effective statutes not only grant authorization for specific actions but also offer comprehensive guidance on executing the authorized action. The proposed statute makes a commendable step toward governing SLED's

223. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring).

224. *See id.*

225. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 359 (4th Cir. 2021) (Wilkinson, J., dissenting).

226. *Jones*, 556 U.S. at 429 (Alito, J., concurring).

227. *Automated License Plate Readers: State Statutes*, NAT'L CONFERENCE OF STATE LEGIS. (Feb. 3, 2022), https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes [https://perma.cc/2RDG-38N3].

228. *Id.*

229. *See id.*

230. *See* H.R. 3374, 2023–2024 Gen. Assemb., 125th Sess. (S.C. 2023).

231. H.R. 3374(E).

utilization of ALPR data insomuch as it provides explicit statutory authorization, thereby alleviating the ultra vires concern at the heart of SCPIF's complaint.[232] However, the proposed statute falls short in actively regulating SLED's use of the ALPR database.

A restriction on data retention fails to address the actual concerns articulated by the Court in *Carpenter*. *Carpenter*'s ruling was unequivocal: a search occurred when "the government *accessed* CSLI from the wireless carriers."[233] Thus, the Court's focus was not on data collection but rather on its utilization.[234] As a result, the absence of practical constraints on law enforcement's surveillance remains of consequence, as surveilling a suspect over a ninety-day period would be nearly impossible without modern surveillance technology. Additionally, retaining ninety days' worth of data provides ample information for law enforcement to glean insights into the private aspects of individuals' lives, especially considering the habitual nature of human behavior. Furthermore, a ninety-day retention policy only has a marginal impact on the overall retrospective nature of ALPR data, as law enforcement can still "travel back in time to retrace a person's whereabouts"[235] well beyond the "4-week mark."[236] Therefore, the South Carolina legislature should exercise its institutional advantages to codify the solution proposed by this Note, which, as previously discussed, avoids the shortcomings associated with regulations on data retention.

While statutory regulation is optimal, it is important to acknowledge its inherent limitations. Namely, the fact that the institutional advantages of legislatures, such as the potential for quicker action compared to courts, often go unrealized.[237] This unrealized potential is partly a product of divisions along party lines, which stall legislative progress. Additionally, legislative decisions are susceptible to political fluctuations; measures passed by one party may be quickly repealed when the opposing party assumes power after an election. The South Carolina ALPR bill exemplifies these limitations, as the same bill has been proposed as early as 2018 and has yet to make it out of the Committee on Judiciary.[238] Consequently, the most effective solution may

232. *See* Project Policing, *supra* note 159, at 14.

233. United States v. Carpenter, 585 U.S. 296, 313 (2018).

234. *See id.* at 313–14.

235. *Id.* at 2218.

236. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

237. *See* Alan B. Rosenthal, The State of the Florida Legislature, 14 FLA. ST. U. L. REV. 399, 430 (1986) ("The performance of a legislature depends on capacity, membership, power, politics, and process") *See also* Stephen Chang, *Towards Moderate Teacher Tenure Reform in California: An Efficiency-Effectiveness Framework and the Legacy of Vergara*, 104 CALIF. L. REV. 1503, 1520 (describing courts as useful to "provide the 'political cover' to permit willing policymakers to act" and to solve legislative log jams).

238. *See generally* H.R. 3366, 2023–2024 Gen. Assemb., 125th Reg. Sess. (S.C. 2023).

be for SLED to undertake self-regulation of its Back Office use—the very matter currently under litigation.[239]

C. SLED Self-Regulation

Just as privacy interests should not be subject to the whims of political majorities, SLED's policing efforts should not be susceptible to the uncertainties of the law. Unlike elected officials, the personnel of administrative agencies, such as SLED, operate independently from political pressures.[240] As a consequence, these agencies possess the capacity to enact regulations with greater agility than legislative bodies. Presently, administrative agencies surpass both Congress and the judiciary in rule creation.[241] Hence, SLED can leverage its rule-making authority to proactively address and preempt any Fourth Amendment challenges to its ALPR utilization.

While the absence of explicit court or legislative directives makes imposing constraints on ALPR usage appear counterintuitive, it is actually advantageous for SLED to adopt a more rigorous regulatory approach to its ALPR usage. Qualified immunity acts to shield law enforcement from legal consequences, leaving the exclusionary rule as the primary recourse for addressing unreasonable searches in violation of the Fourth Amendment.[242] This rule bars the government from introducing evidence obtained in violation of the Fourth Amendment.[243] Consequently, the ambiguous legality surrounding SLED's utilization of ALPR data places the agency at a perpetual risk of having evidence derived from such data suppressed. This risk, in turn, could prove detrimental to SLED's ability to secure a conviction if the contested evidence is pivotal to the prosecution's case. Accordingly, it is advisable for SLED to revise its existing ALPR policy to conform with legal standards, thereby mitigating the risk of suppression.

Specifically, SLED should consider integrating into its policy the limitations suggested by this Note. While mandating officers to secure a warrant for accessing ALPR data beyond individual trips will add an additional hurdle to SLED's policing efforts, incorporating a warrant requirement in the context of ALPR data is not as burdensome as it may initially seem. As previously noted, the Court in *Carpenter* was not concerned

239. *See* Project Policing, *supra* note 159, at 2.

240. NANCY K. KUBASEK & GARY S. SILVERMAN, ENVIRONMENTAL LAW (Prentice Hall 3rd ed. 2000).

241. *Id.*

242. *Exclusionary Rule,* CORNELL L. SCH., https://www.law.cornell.edu/wex/reasonable_suspicion [https://perma.cc/5H38-W9RU].

243. *Id.*

with the existence of the data, only with its use.[244] Thus, a warrant would not be required for the actual collection of ALPR data, allowing SLED to continue aggregating ALPR data from law enforcement agencies across South Carolina without violating the Fourth Amendment. The warrant requirement would become relevant only when an agency seeks access to data beyond that provided by an individual trip.

Secondly, implementing a warrant requirement for data beyond that derived from an individual trip would prevent suppression of ALPR data due to the good-faith exception.[245] This exception ensures that evidence obtained by officers relying on search warrant, even if deemed invalid, is not excluded.[246] Thus, if an officer obtains a warrant to access SLED's ALPR database, any evidence derived from the database will not be suppressed, even if the warrant is ultimately found to be invalid.

Furthermore, implementing a warrant requirement for data beyond that associated with an individual trip is not so rigid as to prevent SLED from using ALPR data when it is absolutely necessary.[247] As the Court in *Carpenter* aptly pointed out, a well-recognized exception to the warrant requirement "applies when 'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment."[248] Such exigencies include "the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence."[249] Thus, when confronted with an urgent situation such as a child abduction, the needs of law enforcement will likely justify an immediate and comprehensive use of the Back Office, obviating the need for a warrant.

Similarly, implementing a reasonable suspicion standard for the warrantless use of the Back Office would not unduly hinder SLED's policing endeavors. For one, the reasonable suspicion standard is likely not much different from SLED's existing restriction, which mandates that the Back Office be used only for "legitimate law enforcement purposes" or "public

244. United States v. Carpenter, 585 U.S. 296, 313-14 (2018).

245. *See* Herring v. United States, 555 U.S. 135, 137 (2009) ("[S]uppression is not an automatic consequence of a Fourth Amendment violation."); *see also* United States v. Leon, 468 U.S. 897, 922 (1984) ("We conclude that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."). *See generally Carpenter*, 585 U.S. at 313–14 (holding that a person has an expectation of privacy in the whole of his or her physical movements, which suggests that accessing such aggregated historical ALPR data beyond an individual trip without a warrant could be considered a violation of the Fourth Amendment).

246. *Exclusionary Rule*, *supra* note 242.

247. *See Carpenter*, 585 U.S. at 319.

248. *Id.*

249. *Id.* at 320.

safety-related missions." Presumably, these restrictions already necessitate an officer to harbor some level of suspicion that a suspect has committed or is about to commit a crime, and that the Back Office contains evidence related to the crime. If so, the current restrictions align closely with the concept of reasonable suspicion, albeit with the distinction that reasonable suspicion demands a suspicion level beyond a mere hunch and requires officers to substantiate their suspicion with articulable facts.[250] Regardless, the ambiguity surrounding SLED's current restriction is a compelling reason for the agency to consider adopting the reasonable suspicion standard. Unlike SLED's current restriction, which lacks a definitive definition, the reasonable suspicion standard is supported by a comprehensive body of case law that clearly outlines the standard, facilitating easier compliance for officers.[251] Additionally, while offering a more precisely articulated standard, reasonable suspicion also grants officers considerable latitude to exercise their professional judgment.[252] Consequently, any supposed benefit SLED gains from maintaining an entirely ambiguous standard becomes inconsequential, as reasonable suspicion enables officers to draw logical inferences based on their experience and expertise.

Moreover, while suppression serves as the traditional remedy for unreasonable searches, suppression is only one reason SLED should be concerned with its current ALPR practices. A Fourth Amendment violation can also give rise to monetary damages via a § 1983 claim.[253] Section 1983 is a federal statute that enables people to sue certain government entities and its employees for violations of their civil rights.[254] Typically, Fourth Amendment violations do not give rise to money damages, as the damage in such cases usually stems from the presentation of illegally obtained evidence; thus, the wrong is generally redressed by suppression of the evidence.[255] However, the existence of § 1983 means that an award of monetary damages is not entirely precluded. Furthermore, whether in defense against a suppression motion or a § 1983 action, the costs associated with litigation are substantial. Therefore, it is in SLED's interest to revise its ALPR policy in accordance with the solution proposed by this Note to prevent an unnecessary expenditure of taxpayer dollars.

---

250. 5 BARBARA E. BERGMAN ET AL., WHARTON'S CRIMINAL PROCEDURE § 29:6 (14th ed. 2023).

251. *See id.*

252. *See id.*

253. *See What are the Elements of a Section 1983 Claim?*, THOMAS REUTERS (June 13, 2022) https://legal.thomsonreuters.com/blog/what-are-the-elements-of-a-section-1983-claim/ [https://perma.cc/3G6L-NJFZ].

254. *Id.*

255. ALLEN ET AL., *supra* note 3, at 317, 331.

V. CONCLUSION

Although no court has explicitly affirmed that the utilization of ALPR databases qualifies as a search under the Fourth Amendment, an application of the Court's reasoning in *Carpenter*, coupled with the state court's hesitancy towards ALPR use, suggests that the utilization of ALPR databases is not entirely immune from Fourth Amendment challenges. Given South Carolina citizens' enhanced Fourth Amendment protection,[256] SLED's use of the Back Office is especially susceptible to such a challenge. Additionally, the Fourth Circuit has already shown a willingness to extend *Carpenter* to "traditional surveillance tools" despite *Carpenter*'s "narrow" holding.[257] Therefore, SLED should proactively address these potential challenges by embracing the solution proposed in this Note, even in the absence of express court or legislative attention to the privacy concerns posed by SLED's ALPR database. By doing so, SLED stands to avoid significant litigation expenses, potential monetary damages awards, and the jeopardization of otherwise straightforward convictions. Importantly, these advantages have a negligible burden on SLED's efficiency, as the proposed solution imposes minimal strain on the agency's existing policing operations.

256. *See* State v. Forrester, 343 S.C. 637, 644, 541 S.E.2d 837, 841 (2001).
257. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021).