6-25-2019

Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy

Lauren Fash

AUTOMATED LICENSE PLATE READERS: THE DIFFICULT BALANCE OF SOLVING CRIME AND PROTECTING INDIVIDUAL PRIVACY

LAUREN FASH*

In 1998, a District of Columbia police lieutenant pleaded guilty "to extorting money from customers of a gay bar."[1] The officer wrote down the license plate numbers of the customers and intimidated them into paying him money by threatening "to expose their lifestyle."[2] Recent developments in technology have automated the process of license plate checking, which has only exacerbated the potential for these types of privacy abuses.[3] Automated license plate readers ("ALPRs") are useful tools for police officers, as they have automated the process of police officers manually scanning license plates and comparing them to police databases.[4] License plate

* J.D. Candidate 2020, University of Maryland Francis King Carey School of Law. The author wishes to thank the *Maryland Law Review* editors for their feedback throughout the revision process as well as Professors David Gray and Mark Graber for their valuable knowledge and insight. The author would also like to thank her parents, Kevin and Boni, for their continuous love and encouragement, and her sister, Madeline for being a constant source of inspiration and joy. The author would like to thank her partner, Will Fitzgerald for his unwavering love, encouragement, and kindness throughout the writing of this Comment and the author's law school journey. Lastly, the author would like to thank her friends, especially Ali Chandler and Christina Martin for all of their support.

1. Josh Hicks, *A Few Reasons the Public Might Care About License-Plate Tracking*, WASH. POST (Feb. 19, 2014), https://www.washingtonpost.com/news/federal-eye/wp/2014/02/19/a-few-reasons-the-public-might-care-about-license-plate-tracking/?utm_term=.ddb15120fc5c.

2. *Id.*

3. *Id.*; *see also* Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ (noting that the Electronic Frontier Foundation discovered that the Oakland Police Department "deployed [license plate readers] disproportionately often in low-income areas and in neighborhoods with high concentrations of African-American and Latino residents").

4. KEITH GIERLACK ET AL., RAND CORP., LICENSE PLATE READERS FOR LAW ENFORCEMENT: OPPORTUNITIES AND OBSTACLES 9 (2014), https://www.rand.org/pubs/research_reports/RR467.html; *see also* DAVID J. ROBERTS & MEGHANN CASANOVA, INT'L ASS'N CHIEFS OF POLICE, AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS: POLICY AND OPERATIONAL GUIDANCE FOR LAW ENFORCEMENT 9 (2012) (finding that ALPR systems have the capabilities to "capture up to 1,800 plates per minute at speeds up to 120–160 miles per hour"); POLICE EXEC. RESEARCH FORUM, HOW ARE INNOVATIONS IN TECHNOLOGY TRANSFORMING POLICING?, 30 (2012), https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf (finding that a recent survey discov-

reader data provides numerous benefits but also has a high potential for abuse.[5] ALPRs are composed of a hardware aspect and a software aspect.[6] The hardware aspect of the device "uses high-speed video cameras" to photograph every passing vehicle, while the software aspect reads and stores the "plate number, . . . date, time and location" of the vehicle.[7]

ALPR devices originated in the United Kingdom as the country sought a way to thwart attacks by the Irish Republican Army ("IRA").[8] Initially, London relied on closed-circuit television to protect the city from the IRA terrorist bombings.[9] The city also installed license plate readers at city entrances to help combat terrorist attacks from the IRA because the IRA routinely used car bombs in the 1990s.[10] Eventually, the United Kingdom developed "Project Laser," a multi-phased effort to equip officers with the resources necessary to identify vehicles and drivers that were "connected with crime, terrorism, and motor vehicle violations."[11] The program was deemed successful as over 46,000 arrests were made because of license plate recognition hits.[12]

In 1998, the technology made its way to North America, with the United States Border Patrol being the first to use the technology in the States.[13] The ALPR technology has enhanced the efficiency of the Immigration and Customs Enforcement Agency—especially as ALPRs are in use at near 100 locations as a way to identify and track vehicles entering the United States.[14] ALPRs have been praised as being effective in "helping to

---

ered officers made "15 total arrests as a result of LPRs, compared to seven arrests resulting from officers doing the manual checks").

5. Hicks, *supra* note 1 (quoting Jack Bernstein, CEO of Locator Technologies, a company involved in ALPR technologies).

6. Shaun B. Spencer, *Data Aggregation and the Fourth Amendment*, J. INTERNET L. 13, 15 (2015).

7. *Id.*

8. Mary Beth Sheridan, *License Plate Readers to Be Used in D.C. Area*, WASH. POST (Aug. 17, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/16/AR2008081602218.html.

9. GIERLACK ET AL., *supra* note 4, at 7.

10. *Id; see also* Tyson E. Hubbard, *Automatic License Plate Recognition: An Exciting New Tool with Potentially Scary Consequences*, SYRACUSE SCI. & TECH. L. REP. 2 (2008), http://jost.syr.edu/wp-content/uploads/automatic-license-plate-recognition_an-exciting-new-law-enforcement-tool-with-potentially-scary-consequences.pdf.

11. ROBERTS & CASANOVA, *supra* note 4, at 6.

12. *Id.*

13. GIERLACK ET AL., *supra* note 4, at 7.

14. David Silverberg, *Automated License Plate Readers on the U.S. Border*, GOVTECH WORKS (Aug. 30, 2017), https://www.govtechworks.com/automated-license-plate-readers-on-the-u-s-border/.

combat the flow of drugs, illegal currency and weapons across the U.S.-Mexico border."[15]

License plate readers' use has increased in number, and the majority of police departments in the United States use these devices.[16] The ALPR devices are an effective way for officers to identify vehicles that are stolen, unregistered, or belong "to sex offenders, crime suspects, fugitives, or amber alert subjects."[17] Because these devices can scan millions of license plates, however, privacy concerns are raised in the data collection and retention of the captured license plate data.[18] Further, searches based on ALPR alerts also raise constitutional concerns.[19] Additionally, few states have passed regulations governing the use of ALPR devices or policies for how the data is to be managed or stored.[20] Although useful, ALPR devices pose a grave threat to constitutional protections—such as the First and Fourth Amendments—if safeguards are not implemented to balance the needs of law enforcement with the right to individual privacy.[21] This Comment will argue that current Fourth Amendment privacy jurisprudence is ineffective at regulating the complexities of automated license plate readers, and that Congress needs to act to ensure privacy rights are protected, while also ensuring law enforcement interests are protected.[22] Part I will trace the history of privacy jurisprudence and highlight recent judicial challenges to ALPR devices. Part II will present elements that are fundamental in any piece of proposed legislation to regulate ALPR devices and explore why Congress is better suited than the individual states or the judiciary to address the concerns raised by ALPR devices.

15. Jordan Steffen, *License Plate Readers Help Police and Border Patrol, but Worry Privacy Advocates*, L.A. TIMES (Dec. 26, 2010), http://articles.latimes.com/2010/dec/26/nation/la-na-license-reader-20101226.

16. *See* Waddell, *supra* note 3 (noting that "a survey of police agencies conducted in 2011 showed that 71 percent of departments used license-plate readers, and that 85 percent of departments planned to increase their use over the next five years").

17. Kimberly J. Winbush, Annotation, *Use of License Plate Readers*, 32 A.L.R. Fed. 7th Art. 8 (2017).

18. Steffen, *supra* note 15. The data set of one company, Vigilant Solutions, "contained more than 3 billion scans, and was growing at a rate of more than 100 million scans a month" as of 2015. Waddell, *supra* note 3. Vigilant Solutions shares their datasets with law enforcement officers. *Id.*

19. 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, 236–38 (2015); Winbush, *supra* note 17, at 8.

20. Dryer & Stroud, *supra* note 19, at 227–28.

21. *See infra* Section II.C.

22. *See infra* Sections II.A–B.

I. BACKGROUND

The data collected and stored by ALPR systems and the stops that are conducted based on ALPR data implicate Fourth Amendment protections.[23] Understanding these implications requires an understanding of how the Fourth Amendment's privacy jurisprudence fits into a world with ever-evolving technology.[24] Additionally, some states have implemented legislation that limits the use of ALPR devices in an effort to protect citizen privacy rights while still allowing police officers to fulfill their law enforcement duties.[25] Section I.A provides an overview of current privacy jurisprudence to demonstrate how ALPRs fit into the current and rapidly changing scheme of technology and Fourth Amendment jurisprudence. Section I.B explores current regulations and legislation being implemented across the nation at the state level and highlights how different states interpret data privacy and the storage of license plate data. Section I.C discusses instances where an alert is sufficient for reasonable suspicion but also reviews the potential for error in ALPR alerts. Section I.D analyzes the privacy implications of stored license plate data and whether the stored data is protected from public release and, if so, the limitations of such protection.

A. An Overview of Current Fourth Amendment Privacy Jurisprudence

In analyzing Fourth Amendment cases, it is necessary to understand the boundaries of privacy protections.[26] In *Katz v. United States*,[27] the defendant made a call from inside a telephone booth where the Federal Bureau of Investigation ("FBI") had attached a listening device to the outside of the booth.[28] In a concurring opinion, Justice Harlan developed a two-part reasonableness inquiry to determine if the defendant had a "constitutionally protected reasonable expectation of privacy" within the telephone booth.[29] The first part of the test looks to see if an individual has "an actual (subjective) expectation of privacy" and the second part focuses on if that expectation is "one that society is prepared to recognize as 'reasonable.'"[30] Justice Harlan explained that even though the defendant was conducting his conversation in public view, he shut the telephone booth door "and pa[id] the

23. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONT. amend. VI.

24. *See infra* Section I.A.

25. *See infra* Section I.B.

26. Katz v. United States, 389 U.S. 347 (1967).

27. 389 U.S. 347 (1967).

28. *Id.* at 348.

29. *Id.* at 360 (Harlan, J., concurring).

30. *Id.* at 361. This test was later adopted by the Court in *Smith v. Maryland*. 442 U.S. 735 (1979).

toll that permit[ted] him to place a call" thus the defendant could have reasonably expected his telephone conversation to have remained private.[31]

In *Kyllo v. United States*,[32] the Court considered whether law enforcement's use of a "thermal-imaging device . . . to detect relative amounts of heat within the home" was a search that violated the Fourth Amendment.[33] This device afforded law enforcement the opportunity "to detect infrared radiation," which is emitted by almost every object, but is invisible "to the naked eye."[34] A United States Department of Interior agent suspected the petitioner, Kyllo, was growing marijuana inside his home, so officers used the device to take two scans of Kyllo's home.[35] The scan revealed that some parts of the house were "relatively" warmer than other parts of the house and warmer than other homes in the complex.[36] The Court held that the use of the thermal imaging device to scan the home was a Fourth Amendment search because the officers used sensory-enhancing technology to discover information that otherwise would not have been known without actual intrusion into the most protected sphere, the home.[37] Further, the Court explained that the Fourth Amendment needs to be interpreted in a manner that can serve both "public interests" and "the interests and rights of individual citizens."[38] Although the thermal imaging technology "was relatively crude," the Court's rule accounted for the "more sophisticated systems" that have since been developed or are in the process of being developed.[39]

With the increase in technological capabilities, courts have addressed questions as to when a search has been conducted using technology, and if that search was reasonable.[40] In *Naperville Smart Meter Awareness v. City of Naperville*,[41] for example, the City of Naperville received 11 million dollars to upgrade their energy grid in 2009, allowing them to replace their old

31. Justice Harlan noted that a telephone booth "is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.* at 361.

32. 533 U.S. 27 (2001).

33. *Id.* at 29.

34. *Id.* Cultivating marijuana indoors requires a significant amount of heat lamps emitting a high intensity of heat to ensure the plants are able to thrive. *Id.*

35. *Id.*

36. *Id.* at 30.

37. *Id.* at 40.

38. *Id.* at 40 (citing Carroll v. United States, 267 U.S. 132, 149 (1925)).

39. *Id.* at 36. The Court further noted, "[I]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Id.* at 33–34.

40. *See e.g.*, Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).

41. *Id.*

analog energy readers with digitized smart meters.[42] These new smart meters collected data every fifteen minutes—registering the amount of electricity that was being used inside a home and how often it was being used.[43] The United States Court of Appeals for the Seventh Circuit held that the public utility's collection of residents' energy usage every fifteen minutes was a search, but it was reasonable because the data was collected to advance public purposes.[44] The court explained, "The touchstone of the Fourth Amendment is reasonableness."[45] As such, the court assessed whether the search was reasonable by balancing the privacy intrusion on the individual against the policy interests advanced by the government.[46] The Court stated individuals "have a privacy interest in their energy-consumption," but because the public utility was collecting the data and not law enforcement, law enforcement could not easily access records of an individual's energy consumption.[47]

The Supreme Court has also considered whether the attachment of a global-positioning-system ("GPS") to an individual's vehicle is a search under the Fourth Amendment.[48] In *United States v. Jones*,[49] the defendant was under suspicion for trafficking narcotics.[50] A joint task-force between the FBI and Metropolitan Police Department targeted the defendant using a variety of surveillance tactics, such as visual surveillance, video surveillance, pen registers, and wiretapping the defendant's cell phone.[51] The information obtained from these surveillance techniques led the government to apply for a warrant for the purpose of placing an "electronic tracking device" on the defendant's vehicle, which was registered to his wife.[52] In the four weeks this device was attached to the vehicle, over 2000 pages of data were generated.[53] The Court held that installing the GPS device on the vehicle and using the device to track the defendant's movements was a search under the Fourth Amendment.[54] The Court clarified that the device granted

42. *Id.* at 524.

43. *Id.*

44. *Id.* at 527–28.

45. *Id.* at 528 (quoting Florida v. Jimeno, 500 U.S. 248, 250 (1991)).

46. *Id.* at 528 (citing Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 187–88 (2004)).

47. *Id.*

48. United States v. Jones, 565 U.S. 400 (2012).

49. *Id.*

50. *Id.* at 403. The defendant was charged with "conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base." *Id.*

51. *Id.*

52. *Id.* The warrant required that the device be installed within ten days of approval, but the warrant was installed on the eleventh day and outside of the District of Columbia. *Id.*

53. *Id.* at 403.

54. *Id.* at 404.

the government the opportunity to "physically occup[y] private property for the purpose of" gathering relevant information related to the investigation.[55]

The Supreme Court recently analyzed how to apply the Fourth Amendment to cell site location signals that had been collected over time and if the government needed a warrant to obtain this information.[56] In *Carpenter v. United States*,[57] the government used the Stored Communications Act[58] to access the defendant's cell phone records.[59] The defendant was charged with robbery and carrying a firearm, and the government sought the cell site location information from the four-month period during which the robberies had occurred.[60] The Court concluded that the government's access to the cell site location information was a Fourth Amendment search because reasonable expectations of privacy extend to a person's "physical movements as captured through" cell site location information.[61] Further, the Court noted that because obtaining these records was a search, a warrant was necessary.[62] The Court explained it was unwilling to "grant the state unrestricted access to a wireless carrier's database of physical location information."[63] It noted that the rule it was adopting took into consideration the growth of modern technology.[64] The Court noted that this case was "not about 'using a phone' or a person's movement at a particular time," but rather this case was about the signals that created "a detailed chronicle of a person's physical presence compiled every day, every movement, over several years."[65]

55. *Id.*

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

57. 138 S. Ct. 2206 (2018).

58. 18 U.S.C. § 2703 (2012).

59. This statute allows the government "to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d) (2012)).

60. *Id.* ("[T]he government obtained 12,898 location points cataloging [defendant's] movements—an average of 101 data points per day.").

61. *Id.* at 2217. The Court explained that prior to the digital age, society would not have expected law enforcement to be able to "secretly monitor and catalogue every single movement of an individual's car for a very long period" (citing United States v. Jones, 565 U.S. 400, 430 (Alito, J., concurring)). *Id*.

62. *Id*. at 2221.

63. *Id.* at 2223. The Court elaborated that "the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities." *Id.* Yet, "this tool risks Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent." *Id.*

64. *Id.* at 2218 (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

65. *Id.* at 2220. The Court also clarified that cell phone location information is not shared voluntarily because cell phones maintain such a vital role in society, explaining that "carrying one is indispensable to participation in modern society." *Id.* (quoting Riley v. California, 134 S. Ct. 2473, 2484 (1914)).

B. The Legislative Shaping of ALPR Boundaries

As the number of license plate reader systems used by law enforcement agencies continues to grow, some state legislatures have developed legislative solutions to prevent the misuse of the data, provided public oversight, and regulated the type of data that can be collected and stored.[66] Many states have also included measures regarding the length of time that data can be stored, ranging from days to months to years.[67] New Hampshire, for example, has one of the shortest retention policies—while Colorado and Georgia have two of the longest.[68]

Both New Hampshire and Montana have included in their legislation standards for what constitutes reasonable suspicion based on ALPR alerts.[69] In Montana, an officer "shall develop independent reasonable suspicion for the stop" or visually confirm the plate matches the alert.[70] Similar to Montana, New Hampshire requires officers to independently develop reasonable suspicion or make a visual confirmation of the plate number.[71] However, New Hampshire also requires that if the plates do match, then the officer should also make an inquiry into the National Crime Information Center Database.[72]

In an effort to protect privacy, some states have attempted to establish a system that allows the public to gain insight into the functionality and the use of ALPR devices in that state, either in the form of statistical analysis or public logs.[73] Other states require independent audits or reports to be made

66. See *infra* notes 76–80 and accompanying text.

67. *See, e.g.*, MONT. CODE ANN. § 46-5-118(1) (2017) (prohibiting the storage of captured plate data for longer than 90 days); MINN. STAT. § 13.824(3)(a) (2015) (restricting the storage of data for more than 60 days from the date of collection); CAL. VEH. CODE § 2413(b) (2011) (limiting the storage of data to 60 days); N.C. GEN. STAT. § 20-183.32 (2015) (limiting captured data to 90 days); UTAH CODE ANN. § 41-6a-2004(1)(c) (2014) (allowing data to be stored for up to nine months); ARK. CODE ANN. § 12-12-1804(a) (2016) (stating that ALPR data "shall not be preserved for more than one hundred fifty (150) days").

68. *Compare* N.H. REV. STAT. ANN. § 261:75-b(VIII) (2017) (stating that collected license plate reads must be deleted within three minutes of being captured, "unless an alarm resulted in an arrest, a citation, or protective custody, or identified a vehicle that was the subject of a missing person or wanted broadcast"), *and* ME. STAT. tit. 29-A, § 2117-A(5) (2009) (stating that scans that "are not considered intelligence . . . investigative record[s] . . . or data collected for the purposes of commercial motor vehicle screening, [and] may not be stored for more than 21 days"), *with* COLO. REV. STAT. ANN. § 24-72-113(2)(a) (West 2015) (requiring data to be deleted after three years) *and* NEB. REV. STAT. § 60-3204(1) (2018) (restricting the storage of data to no more than 180 days).

69. MONT. CODE ANN. § 46-5-117(vi)(A–B); N.H. REV. STAT. ANN. § 261:75-b(VI).

70. MONT. CODE ANN. § 46-5-117(vi)(A–B).

71. N.H. REV. STAT. ANN. § 261:75-b(VI–VII).

72. *Id.*

73. *See* MINN. STAT. ANN. § 13.824(5)(a)(1–4) (West 2015) (requiring a public log to be maintained, including "specific times of day the reader actively collected data; the aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal databases with which the data were compared, unless the existence of

to the legislative body each year.[74] These audits can be used to identify patterns of noncompliance in law enforcement departments.[75]

Several states have also explicitly defined who may access the database.[76] For example, Maryland restricts access to captured plate data unless the law enforcement agency has a "legitimate law enforcement purpose" for utilizing the data collected.[77] Many states have also included limitations on how the data can be used in an attempt to ensure the privacy of the data being collected.[78] As an example, Arkansas limits the use of license plate readers to state, county, or municipal law enforcement agencies for the purpose of comparing "captured plate data with data held by the Office of Motor Vehicle, the Arkansas Crime Information Center [and] the National Crime Information Center."[79] In contrast, Oklahoma authorizes law enforcement departments to use ALPRs "to access and collect data for the in-

the database itself is not public") *and* ARK. CODE ANN. § 12-12-1805(a)(1–2) (2013) (requiring any entity using an ALPR system to "[c]ompile statistical data" that is to be made into a format where the general public can review the data, which is to be preserved for eighteen months).

74. *See* CAL. VEH. CODE § 2413(e) (West 2011) (mandating that the California Highway Patrol monitors the ALPR system to ensure that there is no unauthorized access and requiring annual reports to be submitted to the California legislature outlining the "number of LPR data disclosures, a record of the agencies to which data was disclosed and for what purpose, and any changes in policy that affect privacy concerns"); MD. CODE ANN., PUB. SAFETY § 3-509(e)(1–6) (Supp. 2018) (requiring the Department of State Police and the Maryland Coordination and Analysis Center to report "to the Senate Judicial Proceedings Committee, the House Judiciary Committee, and the Legislative Policy Committee," the number of ALPR devices used in the state, the number of devices submitting data to the Center, the number of retained readings, the number of requests for data, data breaches or unauthorized uses, and a list of the completed audits).

75. *See* MINN. STAT. § 13.824(6)(b) (noting that "[t]he results of the audit are public . . . [and i]f the commissioner determines that there is a pattern of substantial noncompliance . . . by the law enforcement agency, the agency must immediately suspend operation of all automated license plate reader devices until the commissioner has authorized the agency to reinstate their use").

76. *See* MONT. CODE ANN. § 46-5-117(2)(a)(i–ii) (stating that the Department of Transportation or an incorporated city or town "may use a license plate reader" for the purpose of collecting data for planning or regulating parking in a parking system); ME. STAT. tit. 29, § 2117-A(3)(A–C) (2013) (allowing the Department of Transportation, Department of Public Safety, Bureau of State Police and "[a]ny state, county or municipal law enforcement agency" to use automated license plate readers for specific purposes).

77. MD. CODE ANN., PUB. SAFETY § 3-509(b)(1); *see also* MONT. CODE ANN. § 46-5-117(v)(A–G) (requiring law enforcement to use ALPR devices "only to scan, detect, and identify a license plate number for the purpose of identifying" vehicles associated with a crime).

78. *See* ME. STAT. tit. 29, § 2117-A(4) (classifying the collected data as confidential so that it can only be used by law enforcement to "carry[] out its functions or by an agency collecting information . . . for its intended purpose"); N.H. REV. STAT. ANN. § 261:75-b(1) (2016) (stating that an ALPR "shall be installed for the sole purpose of recording and checking license plates and shall not be capable of photographing or recording or producing images of the occupants of a motor vehicle").

79. ARK. CODE ANN. § 12-12-1803(b)(1) (2013); *see also* UTAH CODE ANN. § 41-6a-2003(2)(a) (stating ALPR devices can be used "by a law enforcement agency for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws").

vestigation, detection, analysis or enforcement of Oklahoma's Compulsory Insurance Law."[80]

As license plate reader technology continues to develop, states have sought to draft guidelines on how these devices can be used in a way that will preserve the goals of law enforcement, but also ensure that individual privacy will not be infringed.[81] These trends, however, have only started to begin to develop in states through piecemeal legislation, and even in the 2019 state legislative sessions, only two states have proposed ALPR regulations.[82] While the proposed and enacted legislative pieces are an important step, federal legislation in this area can lead to more widespread regulations protecting individual privacy.[83]

C. ALPR Alerts Are Sufficient to Establish Reasonable Suspicion But Are Not Immune from Error

While only two states have explicitly defined what constitutes reasonable suspicion for ALPR alerts, several state courts have considered whether license plate reader system alerts are sufficient to establish reasonable suspicion for a traffic stop.[84] Generally, an officer can make a traffic stop if the officer reasonably believes that criminal activity "may be afoot."[85] In *Traft v. Commonwealth*,[86] the defendant was operating his vehicle on a public road when an ALPR device that was mounted on an officer's vehicle read his license plate.[87] The officer was alerted that the registered owner of the vehicle was the subject of a warrant for failure to appear in court.[88]

The Kentucky Supreme Court analyzed whether the defendant had a reasonable expectation of privacy in either his license plate or the information the officer obtained from the ALPR alert.[89] The *Traft* court relied on the two-part test developed in *Katz* to conclude that the State did not violate defendant's Fourth Amendment protections because the defendant did

80. 47 OKLA. STAT. tit. 47, § 7-606.1(C)(1) (2017).

81. *See supra* notes 67–68 and accompanying text.

82. *See, e.g.*, S. 40, 2019–2020 Leg., Reg. Sess. (N.Y. 2019) (limiting the use of ALPR devices to state and local law enforcement departments and establishing that data cannot "be used or shared for any other purpose and shall not be preserved for more than one hundred eighty days"); H.R. 73, 2019 Leg., Reg. Sess. (Miss. 2019) (proposing a bill that authorizes a law enforcement officer to use "the motor vehicle insurance verification system to enforce motor vehicle liability insurance" and noting that an officer can only use the verification system to conduct a stop, but cannot use the system to stop a person to conduct a traffic stop unless the officer has reasonable suspicion other laws have been violated).

83. *See infra* Section II.C.

84. Traft v. Commonwealth, 539 S.W.3d 647 (Ky. 2018).

85. Terry v. Ohio, 392 U.S. 1, 30 (1968).

86. 539 S.W.3d 647 (Ky. 2018).

87. *Id.* at 648.

88. *Id.*

89. *Id.* at 649.

not have a reasonable expectation of privacy in his license plate.[90] There was no reasonable expectation of privacy because the license plate was displayed on the outside of his vehicle, as required by law.[91] Although the defendant argued that his warrant was "protected information," the court concluded that it was simply public record.[92] Therefore, an active warrant against the owner of a vehicle is sufficient to establish the necessary reasonable suspicion needed to conduct a traffic stop.[93] The court continued, explaining the ALPR read of the license plate constituted no constitutional violation of any reasonable expectation of privacy because there is no expectation of privacy in a publicly displayed license plate.[94]

The United States Court of Appeals for the Ninth Circuit has also considered the potential for error and misuse that could arise in using ALPR devices to aid law enforcement.[95] In *Green v. City of San Francisco*,[96] the appellant was operating her 1992 burgundy Lexus with license plate number "5SOW350" in San Francisco at night. [97] At approximately 11:15 p.m., her license plate was misread by an ALPR system, causing her vehicle to be mistakenly identified as stolen.[98] Another officer observed the appellant's vehicle pass him and noticed the first three numbers of the license plate matched the description to both the license plate and the vehicle description that had been dispatched over the radio.[99] The officer followed the appellant and stopped her, but at no point did he "visually confirm" the license

90. *Id.*

91. *Id.*

92. *Id.* at 650.

93. *Id.* at 651.

94. *Id.*; *see also* United States v. Williams, 796 F.3d 951, 957–58 (8th Cir. 2015) (finding the officer had reasonable suspicion in part because the ALPR system automated what could otherwise be done manually either through typing the numbers into a law-enforcement database or contacting dispatch to confirm); Hernandez-Lopez v. State, 738 S.E.2d 116, 118–19 (Ga. App. 2013) (holding the officer had reasonable suspicion based on the ALPR alert in part because the ALPR system "merely aided the officer by augmenting his sensory faculties, providing an enhanced ability to process tag information through a law-enforcement database"); Hill v. State, 743 S.E.2d 489, 491 (Ga. App. 2013) ("[V]isual surveillance of vehicles in plain view does not constitute an unreasonable search for Fourth Amendment purposes, even if the surveillance is aided by an officer's use of a license plate tag reader, because a defendant does not have a reasonable expectation of privacy in a plainly visible license plate").

95. Green v. City of San Francisco, 751 F.3d 1039, 1041 (9th Cir. 2014).

96. 751 F.3d 1039 (9th Cir. 2014).

97. *Id.* at 1042.

98. *Id.* The officers whose ALPR system misread the license plate were unable to read the ALPR photograph or "get a direct visual of [the appellant's] license plate." *Id.* Because the officers had a suspect in custody, they dispatched the hit over the radio in case other officers nearby could respond. *Id.* at 1042–43. The officers read the license plate identified by the ALPR system as "5SOW750," describing the vehicle as a "dark Lexus." *Id.* at 1043. However, the radioing officer did not indicate whether he had visually confirmed the license plate matched the ALPR alert. *Id.*

99. *Id.*

plate number, despite the fact "nothing obscured his ability to do so."[100] The court held in part that it could not be established as a matter of law that the officer had sufficient reasonable suspicion to stop the vehicle.[101] The court explained that the San Francisco Police Department did not have any policy specifying whether the camera car operator was solely responsible for ensuring that the ALPR read was accurate.[102] The court elaborated that the facts were in dispute as to whether or not the officer "could reasonably rely on a *lack* of qualifying information from the camera car operator" to support a decision to stop the vehicle without the officer conducting his own "independent verification" of the license plate.[103]

Many state courts have found that ALPR alerts are sufficient to establish reasonable suspicion, but there are still situations where the ALPR alert is not enough for reasonable suspicion and the officer needs to take confirmation steps before initiating a traffic stop.[104] Further, states enacting legislation with guidelines for when an ALPR alert constitutes reasonable suspicion highlights the importance of ensuring officers are stopping the correct vehicles.[105]

D. Privacy Implications of License Plate Data Storage

The Virginia Supreme Court recently distinguished license plate numbers from the actual personal information that is associated with the license plate data collected by an ALPR device.[106] In *Neal v. Fairfax County Police Department*,[107] the petitioner submitted a Freedom of Information Act request to the Fairfax County Police Department seeking the automated license plate reader records for his vehicle.[108] The petitioner sought to end the police department practice of passively collecting and storing the license plate data of individuals that were under no suspicion of criminal activity.[109] The Virginia Supreme Court analyzed whether the information that was being stored by the police department violated the state's Data Collec-

100. *Id.* at 1043. The officer also did not confirm the plate number with dispatch. *Id.*

101. *Id.* at 1046.

102. *Id. But see* People v. Davila, 901 N.Y.S.2d 787 (N.Y. Sup. Ct. 2010) (holding the officer did have reasonable suspicion to stop the defendant's vehicle based on the ALPR alert in part because the department's guidelines were not law, but simply recommendations and the officer was not required to perform the steps in order for reasonable suspicion to exist).

103. *Id.* at 1046.

104. *See* note 97 and accompanying text. *But see* notes 95–102 and accompanying text.

105. *See* text accompanying notes 70–72.

106. Neal v. Fairfax Cty. Police Dept., 812 S.E.2d 444 (Va. 2018).

107. 812 S.E.2d 444 (Va. 2018).

108. *Id.* at 445.

109. *Id.* at 446. The practice the petitioner aimed to stop is known as the passive collection of data. *Id.* In contrast, "active use" refers to running "real time check[s] of license plate numbers against a 'hot list' of license plate numbers to quickly identify vehicles that have been reported stolen, missing, or suspected of involvement in a crime." *Id.* at 446 n.1.

tion Act.[110] The court held that the license plate numbers that were stored in the ALPR database were not personal information as per the Data Collection Act, but the pictures and data associated with each license plate number were personal information.[111] The court reasoned that license plate numbers do "not describe, locate or index anything about an individual."[112] As for the data and images associated with the plate number, the court explained that the "images of the vehicle, its license plate, and the vehicle's immediate surroundings, along with the GPS location, time, and date when the image was captured," allows for inferences to be made about the individual owner of the vehicle regarding their daily activities, routes, or any other information that may be gleaned from having access to those types of records. [113]

The United States District Court for the Southern District of New York has also considered the potential impact of releasing information about the functioning of license plate readers and their locations.[114] In *New York Civil Liberties Union v. Department of Homeland Security*,[115] the plaintiffs sought data through a Freedom of Information Act request to the Department of Homeland Security.[116] The State argued that while it was public knowledge that these cameras were placed throughout Lower Manhattan, revealing the specific camera locations would allow criminals to identify ways to "evad[e] detection and . . . circumvent[] the law."[117] The court denied the release of the documents, holding that the capabilities of these devices are "generally known," but the functionalities and the abilities that these devices have, such as how they transmit data, are unknown.[118] The court elaborated that releasing details about the specifics of the devices

110. *Id.* at 446. The purpose of the Data Act is to "'preserve the rights guaranteed a citizen in a free society' by 'establish[ing] procedures to govern information systems containing records on individuals.'" *Id.* at 448 (alteration in original) (quoting VA. CODE ANN. § 2.2-3800(B)(4) (2018)).

111. *Id.*

112. *Id.* at 450. Additionally, license plate numbers only identify the owner of the vehicle, which may not always be an individual. *Id.*

113. *Id.* (quoting VA. CODE ANN. § 2.2-3801 (2018)). The Court also emphasized that the classification of pictures and associated data as personal information was "consistent with the legislature's intent to remedy the potential mischief posed by 'the extensive collection, maintenance, use and dissemination of personal information.'" *Id.* (quoting VA. CODE ANN. § 2.2-3800(B)(1)).

114. N.Y. Civil Liberties Union v. Dep't of Homeland Sec., 771 F. Supp. 2d 289 (S.D.N.Y. 2011).

115. 771 F. Supp. 2d 289 (S.D.N.Y. 2011).

116. *Id.* at 290. They requested the release of documents that were related to the Lower Manhattan Security Initiative. *Id.*

117. *Id.* at 292.

118. *Id.*

could allow criminals to "identify limitations" and exploit vulnerabilities in the devices. [119]

The Supreme Court of California has also clarified the difference between collecting data for the pure purpose of collecting license plate information and collecting data for use in a criminal investigation.[120] In *American Civil Liberties Union Foundation of Southern California v. Superior Court of Los Angeles County*,[121] the petitioners sought data over a one-week period from the Los Angeles Sheriff's Department and the Los Angeles Police Department.[122] The court held that the indiscriminate scanning of license plates did "not produce records of investigations" because the scans were not conducted pursuant to any inquiries of specific crimes.[123] The court elaborated that plate scans fell into a category of "bulk data collection" even if the scanned plates had the "potential to match a future search query."[124]

As the California Supreme Court noted, ALPR devices have the potential to generate a significant amount of personal information about individuals—prompting concern about the potential intrusions on individual privacy.[125] In *United States v. Jones*, Justice Sotomayor issued a concurrence to express her concerns regarding the increase in the capabilities of technology available to law enforcement and how that prompts reconsideration of the meaning of societal reasonable expectations of privacy.[126] Justice Sotomayor explained that when defining reasonable expectations of privacy, the question to ask should be "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

119. *Id.* Additionally, disclosing this information "could also nullify the deterrent effect created by the absence of information concerning the scope of the surveillance . . . measures." *Id.* at 293.

120. Am. Civil Liberties Union Found. of S. Cal. v. Super. Ct. of L.A. Cty., 400 P.3d 432 (Cal. 2017).

121. 400 P.3d 432 (Cal. 2017).

122. *Id.* at 435. In one week, more than one million license plates had been read. *Id.* The purpose of the request was to examine "the legal and policy implications of the government's use of ALPRs to collect vast amounts of information on almost exclusively law-abiding [citizens of Los Angeles]." *Id.* at 434 (alteration in original) (quoting the petitioners' request for ALPR data through the California Public Records Act). The Los Angeles Police Department retains the information for five years, whereas Los Angeles Sheriff's Department retains the information for two years. *Id.* at 435.

123. *Id.* at 438.

124. *Id.* at 438. The Court acknowledged that bulk collection of data is not exempt but remanded the issue of anonymization and redaction of the plate data to the trial court to determine how the data should be disclosed. *Id.* at 442.

125. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); United States v. Ellison, 462 F.3d 557, 567 (6th Cir. 2006) (Moore, J., dissenting).

126. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

beliefs, sexual habits, and so on."[127] Further, she noted that as society becomes more aware of the various abilities of the government to "watch" citizens, then this action has the potential to "chill[] associational and expressive freedoms."[128]

Justice Sotomayor further noted that if the government is unrestrained in its abilities to collect the most "private aspects of [personal] identity," this can lead to the data being "susceptible to abuse."[129] As noted in both *Neal* and *American Civil Liberties Union Foundation of Southern California*, ALPR devices have the ability to aggregate large amounts of data that can reveal intimate details about individuals.[130] Justice Sotomayor also wrote, "The Government can store . . . records and efficiently mine them for information years into the future."[131] Justice Sotomayor's concern was more than just theory: in *American Civil Liberties Union Foundation of Southern California*, the Los Angeles Police Department primarily collected and retained license plate reader data because of the potential it had to match a future crime inquiry.[132]

Additionally, even though individuals generally do not have a reasonable expectation of privacy in their license plates, there is still a potential for privacy intrusions based on how the license plate data is stored and used.[133] In *United States v. Ellison*,[134] Judge Moore, of the Sixth Circuit, dissented to discuss the Fourth Amendment concerns that arise with the use of ALPR devices.[135] Judge Moore noted, "the constitutional concerns regarding abuse of discretion do not disappear simply because the drivers are not stopped."[136] In particular, she noted there is a serious psychological invasion associated with the knowledge that police officers are able to search "one's personal information . . . for no reason, at any time one is driving."[137] Additionally, she highlighted the potential for error that is inherent with technology, such as computer errors that may result in drivers being

127. *Id.* at 416–17 (noting that a goal of the Fourth Amendment is "to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance'" (citing United States v. Di Re, 332 U.S. 581, 595 (1948))).

128. *Id.* at 416.

129. *Id.* (noting "[t]he net result [of] GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring))).

130. *See* text accompanying *supra* notes 116 and 121–124 (noting the details that can be revealed about individuals when ALPR devices are deployed in large numbers in communities).

131. *Jones*, 565 U.S. at 415.

132. Am. Civil Liberties Union Found. of S. Cal. v. Superior Court of Los Angeles Cty., 400 P.3d 432, 438 (Cal. 2017).

133. United States v. Ellison, 462 F.3d 557, 567 (6th Cir. 2006) (Moore, J., dissenting).

134. 462 F.3d 557 (6th Cir. 2006).

135. *Id.* at 567 (Moore, J., dissenting).

136. *Id.* at 568.

137. *Id.*

stopped based on inaccurate ALPR data.[138] As society becomes more reliant on the abilities of computers to store and process information more quickly, then that amplifies the potential for error. Therefore, there needs to be a mechanism in place to check these risks to ensure errors are minimal.[139]

II. ANALYSIS

As the number of license plate readers continues to increase, the judiciary is constrained in its ability to address adequately the complex privacy issues that they implicate.[140] Even though license plate readers provide a substantial benefit to law enforcement agencies, that benefit should not come at the cost of individual privacy.[141] Current Fourth Amendment jurisprudence is ineffective at providing a sufficient remedy to protect individual civil liberties that may be infringed upon with the increased usage of ALPR devices.[142] Section II.A argues that the Fourth Amendment jurisprudence is ineffective at addressing the complex privacy issues that arise with cases concerning ALPR devices. Section II.B argues that the legislature is more equipped to implement regulations that balance privacy interests and law enforcement interests. Section II.B also focuses on why Congress is the best arena for a legislative solution to the threats posed by ALPR devices. Section II.C drafts a model statute that includes the different fundamental elements that should be included in ALPR legislation.

A. Current Fourth Amendment Jurisprudence Is Ineffective to Address Complex Privacy Issues

As more agencies gain access to license plate reader data, courts are constrained in applying traditional Fourth Amendment jurisprudence to a complex issue.[143] Current Fourth Amendment doctrine centers on an individual's "subjective" privacy expectations, society's "objective reasonableness" of that privacy expectation, and the degree of privacy intrusion.[144] Current doctrine is a product of Justice Harlan's concurrence in *Katz v. United States*, but it has been criticized for its failure to keep up with the

138. *Id.*

139. *Id.* at 570 (quoting Arizona v. Evans, 514 U.S. 1, 26–27 (1995) (Ginsburg, J., dissenting)) (noting that "inaccurate data can infect not only one agency, but the many agencies that share access to the database").

140. *See infra* Section II.A.

141. *See infra* Section II.B.

142. *See infra* Section II.A.

143. David Gray, *The Fourth Amendment Categorical Imperative*, 116 MICH. L. REV. ONLINE 14, 16–17 (2017).

144. Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L.TECH & POL'Y 281, 283 (2011).

number of technologies that have been introduced to society since the opinion was published.[145] Fourth Amendment privacy jurisprudence is criticized because it has not caught up to the changes in technology and instead focuses on older ideas about the more limited capabilities of "public surveillance technologies."[146] Further, "the warrantless use of most surveillance technologies and the collection of personal data fits comfortably within constitutional doctrine."[147] Technological advancement affords the government with more options to conduct efficient searches, but it does so "on an *almost* unimaginable scale."[148] Essentially, modern judicial interpretations of *Katz* grant the government unlimited authority to conduct searches of public spaces using surveillance cameras, automated license plate readers, drones, and facial recognition technology.[149]

Under the current reading of *Katz*, an individual's license plate is exposed to the public and ALPR devices are operated in areas where an individual has no constitutional right to privacy.[150] ALPR devices read publicly displayed license plates which grants police officers the freedom to investigate people as they expose their vehicles to the public.[151] While the license plates themselves are visible to the public and thus, not subject to any reasonable expectation of privacy, the data associated with the plates, such as where the individual is going, the time of their travel, the routes of their travel, and the pictures of their vehicle and nearby surroundings, are not visible to the public.[152]

The Supreme Court has also long displayed a reluctance to regulate devices that provide a benefit to law enforcement.[153] ALPR devices allow law enforcement to increase efficiency and focus on other areas of crime while still locating criminals quickly.[154] Situations involving "efficiency-enhancing devices" are generally not regulated by the Court, unless it is a device that provides law enforcement with extrasensory abilities.[155]

145. Gray, *supra* note 143, at 15–17.

146. Rushin, *supra* note 144, at 282.

147. *Id.* at 283 ("The recording of a person's movements in public is not especially intrusive and certainly does not provide police with any intrusive, extrasensory abilities beyond mere observation.").

148. Gray, *supra* note 143, at 16 (emphasis added).

149. *Id.* at 16–17.

150. Michael E. Fisher, *Ohio Is Jonesing for Automatic License Plate Readers: Why This May Violate Your Fourth Amendment Rights and What The Ohio Legislature Should Do About It*, 64 CLEV. ST. L. REV. 329, 336 (2016).

151. Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 2–3 (2013).

152. Neal v. Fairfax Cty. Police Dep't, 812 S.E.2d 444, 450 (Va. 2018).

153. Rushin, *supra* note 144, at 305–07; *see also* Rushin, *supra* note 151, at 32 (noting that "[t]he Court has long displayed a reluctance to regulate police efficiency").

154. Rushin, *supra* note 144, at 292–93.

155. Rushin, *supra* note 151, at 32; *see also* Kyllo v. United States 533 U.S. 27, 40 (2001) (holding that when "the Government uses a device that is not in general public use, to explore the

Kyllo v. United States and *Katz* both highlighted the potential for intangible data to be protected by the Court, but ALPR devices are also unique from the wiretapping at issue in *Katz* and the thermo-imaging device at issue in *Kyllo*.[156] ALPR devices are distinct technologies because these devices provide a significant benefit to law enforcement that would otherwise be completed in a much slower fashion.[157] Further, the aggregated data is collected based on an individual driving on public roads where the individual is exposing themselves to the public, which further restricts ALPR devices from sitting comfortably within current doctrine.[158]

Current privacy jurisprudence and its relationship to ALPR devices or other forms of massive data collection have generated concern from Supreme Court Justices, circuit court judges, and other individuals.[159] Notably, in *United States v. Jones*,[160] two Supreme Court justices concurred expressing concern regarding how the most seemingly normal surveillance can result in the collection of massive amounts of data which can lead to a "potentially unconstitutional invasion of individual privacy."[161] Although ALPR devices and GPS devices are different because GPS devices track every single movement whereas ALPR devices are tracking the movement of every single vehicle traveling on a certain road, at a certain time, or in a

details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant").

156. *See supra* text accompanying notes 26–39.

157. *See supra* note 4 and accompanying text (discussing the increased capabilities of law enforcement when ALPR devices are in use).

158. *See infra* notes 159–166 and accompanying text (discussing mass data collection and how it might prompt reconsideration of the notion of a reasonable expectation of privacy).

159. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) ("GPS monitoring is cheap in comparison to conventional surveillance techniques and . . . evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (citing Illinois v. Lidster 540 U.S. 419, 426 (2004))); United States v. Ellison, 462 F.3d 557, 567 (6th Cir. 2006) (Moore, J., dissenting) (noting that the main issue before the court was whether law enforcement can "conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion"); 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/ (explaining that the American Civil Liberties Union obtained documents from the FBI's Office of General Counsel "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"); *see also* notes 125–139 and accompanying text (describing the privacy concerns raised by Justice Sotomayor and Judge Ellison).

160. In this case, the government placed a GPS tracker to the undercarriage of the defendant's wife's vehicle to support the government's case that the defendant was involved in narcotics trafficking. United States v. Jones, 565 U.S. 400, 402–03 (2012).

161. Rushin, *supra* note 151, at 11; *see* Rushin, *supra* note 144, at 308–09 (noting that the Seventh Circuit has stated "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" (quoting United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007)).

certain location.[162] A community with enough ALPR systems, however, "could ultimately create an accurate and pervasive record of a person's movements over months, or even years."[163] Judge Posner of the Seventh Circuit Court of Appeals noted that if the government "someday decide[s] to institute a program of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search."[164]

Technological changes have highlighted the gaps that exist within the *Katz* doctrine because "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."[165] Yet, the expansion of efficiency-enhancing technologies have resulted in the creation of a "digitally efficient investigative state" that has become so intrusive on individual privacy that the Court needs to amend Fourth Amendment jurisprudence to account for the changes in society.[166] With ALPR data, the question becomes whether an individual has a reasonable expectation of privacy in the information associated with their license plate in an aggregated ALPR database.[167] The gaps in current Fourth Amendment jurisprudence created by the "reasonable expectation of privacy test" in *Katz* serve as a barrier to privacy protections when ALPR devices are unregulated because the courts lack the means to develop a sufficient solution.[168] The Supreme Court reviews only the information before it when deciding how to achieve the ideal "constitutional balance" between privacy and liberty, but the Court's limited scope of review constrains the Court into crafting solutions that are within the meaning of the Fourth Amendment.[169]

Recently, in *Carpenter v. United States*, the Supreme Court indicated the potential to expand the definition of privacy to account for changes in technology.[170] The Court took care to ensure that this decision would be narrowly applied to only cell site location information.[171] The Court em-

162. *See supra* notes 120–133 and accompanying text.

163. Rushin, *supra* note 144, at 286.

164. *Garcia*, 474 F.3d at 998.

165. United States v. Jones, 565 U.S. 400, 427 (Alito, J., concurring) (noting that even if people are hesitant to accept the changes in technology that "they may eventually reconcile themselves to this development as inevitable").

166. Rushin, *supra* note 151, at 3.

167. Dryer & Stroud, *supra* note 19, at 237.

168. Laura K. Donohue, *Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 685 (2017); *see also* Rushin, *supra* note 151, at 50 (finding that "[t]he Supreme Court is institutionally limited in its capacity to develop a response to the digitally efficient investigative state").

169. Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 520 (2017); *see infra* note 178.

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

171. *See supra* notes 56–65 and accompanying text.

phasized "the progress of science" has allowed law enforcement to use a "powerful new tool" to carry out law enforcement duties, but at the same time, these new tools create risks that that the Fourth Amendment was designed to prevent.[172] Additionally, the cell site location signals at issue in *Carpenter* are distinct from the data generated by an ALPR device because individuals "regularly leave their vehicles," but a cell phone "faithfully follows its owner beyond public thoroughfares."[173] Although *Carpenter* is useful, the Court was careful to narrowly apply its reasoning only to cell site location information, specifically stating that this decision did not "call into question conventional surveillance techniques and tools, such as security cameras."[174] Nonetheless, privacy advocates, like the American Civil Liberties Union ("ACLU"), viewed the Court's reasoning as "open[ing] the door to the protection of the many other kinds of data generated by popular technologies."[175] The ACLU explained that *Carpenter* could potentially impact government access to various types of "popular technolog[y]" and the information obtained from those technologies.[176]

As society continues to rapidly advance with technology, technology places "privacy and liberty norms in flux" and "police should seek the assistance of legislatures in governing investigatory methods, and they must seek the approval of courts."[177] However, the courts are an arena "of review, not of first view," further limiting their ability to construct adequate solutions to protect individual privacy.[178] The Court is limited by the current doctrine that is incompatible with the rapidly evolving technological state and cannot act on its own to create an effective solution that will be beneficial to both law enforcement and individual privacy interests.[179]

B. The Legislature Needs to Act to Protect Both Privacy and Law Enforcement Interests

Given the existing constraints on the judiciary, the federal legislative branch is in the best position to implement a comprehensive statute that provides a guideline as to how ALPR devices should be regulated to ensure

172. *Carpenter*, 138 S. Ct. at 2223.

173. *Id.* at 2218. The Court also highlighted that government locational tracking "achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.*

174. *Id.* at 2220.

175. Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital* Age, AM. CIV. LIBERTIES UNION (June 22, 2018, 2:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age.

176. *Id.*

177. Henderson, *supra* note 169, at 521 (emphasis omitted).

178. *Id.* at 522; United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) (explaining "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions").

179. Rushin, *supra* note 151, at 4.

that individual privacy interests are respected and that law enforcement is not constrained in their ability to investigate and solve crime.[180] Section II.B.1 discusses the unique challenges associated with ALPR devices, highlighting both the privacy concerns and the interests of law enforcement. Section II.B.2 focuses on how Congress is more equipped than the states to implement a federal statute given the intricacies of ALPR devices and the potential for the data to be transmitted across state lines, thus hindering the effectiveness of any single state regulation or protection on how the data can be used, stored, or accessed.

1. The Creation of a Statutory Scheme Will Require Input from Law Enforcement and Privacy Advocates to Create a Balanced Solution

License plate readers allow law enforcement officers to carry out their duties more efficiently.[181] With this increased efficiency, officers are able to issue more traffic citations, locate stolen vehicles, identify drivers with suspended licenses, and discern vehicles that violate state emission laws.[182] Further, ALPR device surveillance is useful because of its ability to deter illegal behavior.[183] Although ALPR devices increase law enforcement efficiency, other organizations, such as the ACLU and the Electronic Frontier Foundation, have found that ALPR devices amass significant quantities of data, but are not locating vehicles or individuals associated with violent or serious crimes.[184] Law enforcement agencies fear that legislative solutions

180. Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy and Access to Government Information*, 66 ME. L. REV. 397, 432–33 (2014); *see infra* Section II.B.2.

181. *Id.* at 398; *see also* GIERLACK ET AL., *supra* note 4, at 13 (finding that a single officer in Montgomery County, Maryland was able to read "48,000 vehicles in 96-hour periods . . . across 27 days").

182. *See* GIERLACK ET AL., *supra* note 4, at 13 (noting that one Montgomery County, Maryland police officer was able to "issue[] 255 traffic citations, identif[y] 26 drivers with suspended licenses, ca[tch] 16 vehicle-emissions violators, [and] f[i]nd four stolen vehicles"); *see also* ROBERTS & CASANOVA, *supra* note 4, at 23 (reporting that the Automated Regional Justice Information Sharing system conducted a five day test at the United States—Mexico border, where 780,000 plates were read, "and over 1,300 were involved in 4 murders, 14 rapes, 24 robberies, 273 assaults, 128 burglaries, 345 vehicle thefts, 361 weapons, and 241 narcotics cases").

183. *See* Rushin, *supra* note 144, at 297 (finding that individuals will "avoid[] illegal behavior in the vicinity where police surveillance is happening or has occurred, but also avoid[] illegal behavior generally because of the observed surveillance").

184. The ACLU requested the license plate records from Maryland's ALPR database and discovered that of the "over 29 million [plate] reads . . . [o]nly 0.2 percent . . . or about 1 in 500, were hits." AM. CIVIL LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 13 (2013), https://www.aclu.org/other/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements?redirect=technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record [hereinafter YOU ARE BEING TRACKED]. In 2012,

will result in overly burdensome storage limitations, thus undermining the legitimate use of ALPR data and hindering law enforcement's ability to solve crime.[185]

Even though ALPR devices allow officers to carry out their duties more efficiently, the mass aggregation of citizen data poses a threat to individual privacy.[186] The Los Angeles Police Chief has described the "real value [of ALPR]" as coming "from the long-term investigative uses of being able to track [all] vehicles—where they've been and what they've been doing."[187] Decreased data storage costs incentivize law enforcement departments to hold onto ALPR data for longer periods of time.[188] "[H]istorical and psychological evidence," however, has found that unregulated police surveillance has negative consequences.[189] Without legislative protections, the unregulated nature of automated license plate readers "may incentivize police fishing expeditions, facilitate racial profiling, and corrode any notion of public anonymity."[190]

2. Congress Is Better Suited Than the States to Adopt a Comprehensive Statutory Scheme Governing ALPR Devices

Several states have already begun to implement policies related to ALPR devices, but this has been a slow, piecemeal process.[191] In *United States v. Jones*, Justice Alito noted that in situations "involving dramatic technological change, the best solution to privacy concerns may be legislative."[192] As more agencies begin using ALPR devices, the federal legislature is in the strongest position to evaluate competing interests and to ensure ALPR data policy takes into consideration privacy interests and law enforcement interests.[193] This Section explores why Congress is in the best

"[f]or every one million plates read in Maryland, only 47 were potentially associated with more serious crimes." *Id.* at 14.

185. Dryer & Stroud, *supra* note 19, at 228.

186. *See* Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from the Cops*, ARS TECHNICA (Mar. 24, 2015, 9:00 AM), https://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/. A study conducted by ars Technica, in Oakland, CA, found that over 4.6 million scans had been read in three years, leading to 1.1 million unique plates being identified. *Id.* Although many of the plates had only been read a few times, using a "custom-built visualization tool . . . [a]nyone in possession of enough data can often . . . make educated guesses about a target's home or workplace, particularly when someone's movements are consistent." *Id.*

187. Rushin, *supra* note 144, at 286 (alterations in original).

188. GIERLACK ET AL., *supra* note 4, at 19.

189. Rushin, *supra* note 151, at 21; *see also* note 137 and accompanying text (describing the effects of surveillance on human behavior).

190. Rushin, *supra* note 144, at 283; *see also infra* notes 235–241 (discussing the ways law enforcement has used ALPR devices to target certain races and religions).

191. *See supra* Section I.B.

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

193. *Id.*

position and how a comprehensive scheme can be used by the Court to address privacy-related challenges to ALPR devices and the collection of data.

ALPR data is championed by law enforcement as a way to efficiently solve crime, yet criticized by privacy advocates as eroding individual concepts of privacy.[194] Given these competing tensions, Congress is best suited "to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[195] Federal legislators are able to obtain input from a variety of sources, such as "legislative hearings," "poll results" and "interest group advocacy."[196] Additionally, the legislative process is more open and is accompanied by public scrutiny which "tend[s] to ferret out rules that are particularly unbalanced."[197]

A congressional statutory scheme for ALPR data is not unique and would not be the first time that Congress has acted to protect individual privacy.[198] At times, Congress has acted on its own initiative to pass legislation that would protect people from new technologies such as the Privacy Act of 1974,[199] which allowed people to identify incorrect information about themselves in "computer databases."[200] Another example is the federal wiretapping statute where Congress stepped in instead of allowing the courts to "develop a body of Fourth Amendment case law governing that complex subject."[201] Also, Congress does not need to wait until an issue presents itself; Congress has acted on issues, such as creating the Electronic Communications Privacy Act,[202] even before the court had considered whether the Fourth Amendment extends to email privacy.[203] Congress has the tools and the ability to act to protect individual privacy in relation to the aggregation of ALPR data.

A comprehensive congressional statutory scheme would not only provide evidence as to societal expectations about privacy, but it would allow Congress "to regulate both public and private parties to best protect privacy."[204] Congress has the ability to rely on public opinion and other information to craft a multi-dimensional solution that protects individual privacy

194. Dryer & Stroud, *supra* note 19, at 229.

195. *Jones*, 565 U.S., at 429–30.

196. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875 (2004).

197. *Id.* at 881.

198. *Id.* at 871 (explaining that Congress often has the lead with respect to new technology and criminal investigations).

199. 5 U.S.C. § 522(a) (2000).

200. *Id.* at 855.

201. *Jones*, 565 U.S., at 427.

202. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended as a note to 18 U.S.C. § 2510 (2000)).

203. Kerr, *supra* note 196, at 870.

204. *Id.* at 872.

and respects law enforcement.[205] This statutory scheme is also a useful guide for the courts in understanding societal expectations about privacy.[206] A federal legislative statute provides courts with actual evidence of how society feels about technology and its capabilities.[207] A federal legislative solution is also preferable because the Supreme Court favors federal legislation when determining reasonable expectations of privacy.[208] Given the complexity of data privacy and the inconsistences in both state courts and state legislative statutes, Congress needs to act to create a uniform response.[209] A uniform federal response is crucial to protecting individual privacy because it provides a baseline understanding of legislative evidence for the Court to use when considering societal expectations of privacy involving the aggregation of data from law enforcement.[210]

C. A Model Legislative Proposal

With the implementation of ALPR devices in numerous law enforcement agencies, regulations have developed in piecemeal fashion, sometimes with states and jurisdictions adopting no regulations at all.[211] As ALPR devices have the potential to gather mass quantities of personal data regarding an individual's daily activities, however, regulation at the federal level becomes increasingly necessary.[212] Legislative solutions need to consider the inherent challenges associated with ALPR devices while still ensuring that ALPR devices are not rendered ineffective with overly restrictive legisla-

205. *Id.* at 881–82.

206. Colin Shaff, Note, *Is the Court Allergic to* Katz*? Problems Posed by New Methods of Electronic Surveillance to the 'Reasonable-Expectation-of-Privacy" Test*, 23 S. CAL. INTERDISCIPLINARY L.J. 409 (2014).

207. *Id.* at 440 (explaining that the Court shows deference when Congress enacts "'comprehensive' federal legislation" (citing United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring))).

208. *Id.* at 439 (explaining that even when state legislation is "a more accurate representation of [individual privacy expectations]," the Court "tends to disregard state legislation"); *see also* Neil Colman McCabe, *Legislative Facts as Evidence in State Constitutional Search Analysis*, 65 TEMP. L. REV. 1229, 1240 (1992) (noting that "state and local laws cannot serve as legislative facts unless they are representative of a national, rather than merely a statewide, societal understanding").

209. *See supra* Sections I.C–D.

210. *See* California v. Greenwood, 486 U.S. 35, 43 (1987) (explaining that societal expectations of privacy "must turn on such factors as 'our *societal* understanding that certain areas deserve the most scrupulous protection from government invasion'" (quoting Oliver v. United States, 466 U.S. 170, 178 (1984))); *see also* Kerr, *supra* note 196, at 806 (explaining that "legislative privacy rules" have been either as protective or more protective, than "parallel Fourth Amendment rules"); McCabe, *supra* note 208, at 1231 (noting that the Court has considered "legislative or social facts" even if the parties have not presented those facts in arguments). *But see* Shaff, *supra* note 206, at 444–45 (criticizing the federal legislature for failing to update federal privacy laws, thus leaving in place an "outdated understanding of electronic communication").

211. Rushin, *supra* note 144, at 286–87.

212. *See supra* Section II.B.

tion.[213] Section II.C.1 argues determining who has access to the data and how the data can be shared is fundamental to protecting privacy and allowing law enforcement to carry out their duties. Section II.C.2 focuses on the importance of establishing reasonable suspicion guidelines to minimize the risk of error and abuse. Section II.C.3 argues that the lower cost of data storage has served as an incentive for law enforcement agencies to adopt this technology more broadly, but that regulations need to serve as a compromise between citizen privacy and law enforcement investigations. Section II.C.4 discusses the value of public input and audits to ensure that the public and the police force are able to determine that the benefits outweigh the risks.

1. Controlling Access and Sharing Data

As more law enforcement agencies adopt ALPR devices, Congress needs to establish guidance on who can access this information and how it is shared with other agencies.[214] Legislative solutions should require agencies to adopt policies that focus on how the data should be collected and how to use that data in an appropriate manner.[215] Any public entity that relies on ALPR devices should draft regulations identifying the employees who can access the data while also specifying the training these employees need to undergo.[216] Specifically stating who can have access to the data can ensure that the data is being used appropriately and according to the statutory mandate.[217] These regulations should also define the "allowable uses of ALPR technology and data."[218] Additionally, Congress should require law enforcement to make these regulations public to increase transparency and public awareness about how this data is being handled and protected.[219]

American policing is highly decentralized, which has led to an increase in sharing license plate data among different jurisdictions.[220] The main benefit of this decentralized system is that it aids in locating criminals and

213. *See infra* Section II.C.1.

214. Dryer & Stroud, *supra* note 19, at 265–66.

215. INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 48 (2009).

216. Fisher, *supra* note 150, at 349.

217. *Id.*

218. Dryer & Stroud, *supra* note 19, at 265; *see also* MD. CODE ANN., PUB. SAFETY § 3-509(a)(8) (Supp. 2018) (defining "legitimate law enforcement purpose" as "the investigation, detection or analysis of a crime or a violation of the Maryland vehicle laws or the operation of terrorist or missing or endangered persons or alerts"); UTAH CODE ANN. § 41-6a-2003(2)(a) (2014) (restricting the use of ALPR devices to law enforcement agencies "for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws").

219. *See* Fisher, *supra* note 150, at 349 (arguing that granting the public access to training policies increases accountability).

220. Rushin, *supra* note 151, at 12.

stolen property.[221] With the increase in automated license plate readers, the federal government and state government agencies have developed "fusion centers" as a place to store and share data across city and state borders.[222] As the data is shared among state and local governments, the privacy regulations governing in one jurisdiction may no longer apply in another.[223] Agencies that share data with other jurisdictions should work together to create "model memoranda of understanding."[224] These memoranda are used to work out the details as to how to share hotlist data and other related ALPR data.[225] Further, if jurisdictions are sharing data, then they should be transparent about what other jurisdictions or agencies they are sharing the license plate data.[226] Any congressional solution should result in a policy that considers the privacy risks that exist when data is shared with a multitude of other jurisdictions.[227] A federal policy needs to consider both the risks that may be associated with sharing data and be sure to take an affirmative action to protect individual's privacy and ensure jurisdictions and fu-

221. *Id.*

222. Rushin, *supra* note 144, at 292 (explaining fusion centers "were created by Congress as central databases for compiling terrorist-related information that could be shared with local law enforcement"). Fusion Centers allow states and large metropolitan areas to operate as "focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners." *State and Major Urban Area Fusion Centers*, DEP'T OF HOMELAND SECURITY (Aug. 31, 2018), https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

223. Dryer & Stroud, *supra* note 19, at 264–65.

224. GIERLACK ET AL., *supra* note 4, at xiv; *see also Memorandum of Understanding for Sharing Law Enforcement Information*, CITY OF CHENERY 4–6 (2012), https://www.cityofcheney.org/DocumentCenter/View/97/SouthBay-Information-Sharing-System—Law-Enforcement-Information-Sharing (providing an example of a data-sharing Memorandum of Understanding between eight law enforcement departments and the South Bay Information Sharing System).

225. GIERLACK ET AL., *supra* note 4, at 66 (explaining that "[n]egotiating such [memorandums of understanding] with other agencies or jurisdictions can both be time-consuming and troublesome . . . [and that] agencies should consider appending LPR agreements to an existing [memorandum of understanding] related to data-sharing" instead of creating a separate one that is only for ALPR devices); *see also* NAT'L LEAGUE OF CITIES, SHARING DATA FOR BETTER RESULTS 15 (2014), http://www.nlc.org/sites/default/files/2016-12/Data%20Sharing%20for%20Better%20Results.pdf (explaining that a Memorandum of Understanding should include "the agreed upon purpose of the initiative, the human and technological implementation plans, and the agreed upon privacy and security protections associated with an integrated data system").

226. YOU ARE BEING TRACKED, *supra* note 184, at 32.

227. Dryer & Stroud, *supra* note 19, at 265–66; *see also* Andrew Keatts, *SDPD Shares Its License Plate Database with Border Patrol—and Hundreds of Other Agencies*, VOICES OF SAN DIEGO (Apr. 26, 2018), https://www.voiceofsandiego.org/topics/public-safety/sdpd-shares-its-license-plate-database-with-border-patrol-and-hundreds-of-other-agencies/ (noting the San Diego Police Department has admitted to having "broad leeway over who can access the data, and that it has not elected to limit that access" and "[a]gencies that can see the data range from Border Patrol to tiny local police departments across the country").

sion centers are being transparent about how the data is being stored and used.[228]

As part of protecting privacy, statutes need to include guidance to ensure that the data is not being misused and that law enforcement is not using the technology as a means of targeting certain classes of individuals.[229] Legislation targeting law enforcement practices must be easy to interpret and implement in a variety of different circumstances to prevent law enforcement from misunderstanding and misapplying the provisions.[230] Even if the government does not plan to use the collected data, there is still the potential for misuse and the existence of a "chilling effect" on individuals' freedoms.[231] This effect has been noted by the International Chiefs of Police who, in 2009, stated that the unregulated use of ALPR technology may result in the public becoming "more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[232] As then-Governor Bobby Jindal of Louisiana explained, "ALPR systems 'pose a fundamental risk to personal privacy and create large pools of information belonging to law abiding citizens.'"[233] Additionally, a former police chief in Minnesota noted at a city council meeting that ALPR technology is useful and beneficial, but that he did not "want the good guys being kept in a database" even if "it helps catch the bad guys."[234]

Moreover, if individuals are aware that their movements are being tracked, then this could have a potentially "chilling effect" on people exercising their First Amendment rights.[235] The ACLU has noted that the New York City Police Department has driven vehicles around different parts of

228. *See infra* Section II.C.4.

229. Dryer & Stroud, *supra* note 19, at 266; *see also supra* notes 1–3 and accompanying text (describing how a Washington, D.C. police officer relied on license plate numbers to target a specific class of individuals).

230. Rushin, *supra* note 151, at 43–44.

231. YOU ARE BEING TRACKED, *supra* note 184, at 32; *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (describing the potential privacy threats that exist when law enforcement relies on GPS tracking devices to monitor citizens).

232. Jennifer Lynch & Peter Bibring, *Los Angeles Cops Should Release Automatic License Plate Reader Records, EFF & ACLU Argue in Opening Brief*, ELECTRONIC FRONTIER FOUND. (Jan. 28, 2014), https://www.eff.org/deeplinks/2014/01/los-angeles-cops-should-release-automatic-license-plate-reader-records-eff-aclu; *see also* Brief for Electronic Frontier Found. & Brennan Ctr. for Justice at NYU Law School, as Amici Curiae Supporting Appellant at 20–24, Neal v. Fairfax Cty. Police Dep't, 812 S.E.2d 444 (Va. 2018) (noting that the Virginia State Police used ALPR devices to scan the plates of all individuals that attended political rallies for Sarah Palin and Barack Obama and that Immigration and Customs Enforcement has used ALPR devices to gather information about gun show customers).

233. Brief for Electronic Frontier Found. & Brennan Ctr. for Justice, *supra* note 232, at 23 (quoting Bobby Jindal, then-Governor of Louisiana).

234. *Id.* at 22.

235. *Id.* at 20.

the city to use ALPR devices to gather the license plates of individuals who go to mosques.[236] Additionally, Electronic Frontier Foundation found that license plate data obtained from the Oakland Police Department demonstrated that police officers were able to create a grid of the "city's poorest neighborhoods" using collected license plate data. [237] The Oakland data highlighted racial disparity; as vehicles parked or drove through neighborhoods that were predominately white, the vehicles "[were] less likely to be picked up by the ALPR cameras."[238] In contrast, vehicles driving or passing through neighborhoods with a higher black or Hispanic population were more likely to have their plate read by an ALPR device.[239] For this reason, legislation should also include provisions that prevent law enforcement from targeting individuals based on their membership in a protected class.[240] Effective legislation could counter the negative and chilling effect that exists when individuals are aware that their license plates are being tracked.[241] This type of compromise would still allow the government to benefit from the use of ALPR devices to track criminals and prevent crime but also would ensure that citizen privacy is not negatively impacted by the indiscriminate collection of license plate data.[242]

2. Reasonable Suspicion and Reducing Error

Allowing law enforcement to have discretion in choosing when to make a stop or how to carry out their duties is a crucial aspect of policing, but there should still be guidelines in place to ensure that an officer is stopping the correct vehicle for the correct crime to minimize the risk of error.[243] In *Green v. City of San Francisco*,[244] the plaintiff was stopped because her vehicle was thought to be associated with reports of a stolen vehicle.[245] As the plaintiff complied with the officers' orders, at least four

236. YOU ARE BEING TRACKED, *supra* note 184, at 11; *see also* Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, ASSOCIATED PRESS (Feb. 23, 2012), https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques (explaining that "[t]he NYPD Intelligence Division snapped pictures and collected license plate numbers of congregants . . . [and] [p]olice mounted cameras on light poles and aimed them at mosques").

237. Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, ELECTRONIC FRONTIER FOUND. (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

238. *Id.*

239. *Id.*

240. Dryer & Stroud, *supra* note 19, at 245–46.

241. *Id.*

242. Fisher, *supra* note 150, at 349.

243. GIERLACK ET AL., *supra* note 4, at 15 (noting "misreads occur [and] the systems' readers can have difficulty distinguishing between plates from different states").

244. *See supra* notes 95–103 and accompanying text.

245. Green v. City of San Francisco, 751 F.3d 1039, 1043 (9th Cir. 2014).

officers were pointing their weapon towards her.[246] After the plaintiff was subjected to a pat-down search that revealed nothing, the officers "finally" ran the plaintiff's license plate number—finding that her license plate matched her vehicle, which had not been reported stolen.[247] Even though the plaintiff had only been subjected to a pat-down, the experience was nonetheless terrifying and resulted in her attending counseling and missing *several* weeks of work.[248] Instances such as this one highlight the importance of ensuring there is some sort of guidance in place to help mitigate the risk of error.[249]

Establishing guidelines on when an officer can make a stop based on an ALPR alert is one way to ensure that citizens are not wrongfully stopped for crimes they have not committed.[250] Confirming license plate numbers match an active alert for criminal activity is important because hotlists may not always be up-to-date, which may mean a stolen vehicle may have been recovered and the driver of the vehicle is the actual licensed driver.[251] Additionally, there exists the potential for error in the form of misreads by the ALPR device, which only heightens the need for law enforcement to double-check and confirm plate reads before making a stop.[252]

In *Green*, the plaintiff was eventually allowed to leave and law enforcement was deemed to be merely carrying out their duties, but the case highlights a very real issue—ALPR devices provide benefits, but relying too much on quick computer reads can result in traumatic experiences for individuals.[253] Several factors can influence a plate read, such as "vehicle speed," "weather conditions," lighting conditions," or even the "character

246. *Id.*

247. *Id.*

248. Martha Neil, *City Faces Suit over Police Stop Based on License-Plate Reader Error*, A.B.A. J. (June 18, 2014), http://www.abajournal.com/news/article/license-plate_reader/.

249. Jennifer Lynch, *New Ninth Circuit Opinion Calls into Question Blind Reliance on License Plate Camera IDs*, ELECTRONIC FRONTIER FOUND. (May 21, 2014), https://www.eff.org/deeplinks/2014/05/new-ninth-circuit-opinion-calls-question-blind-reliance-license-plate-camera-ids (noting that the International Association of Chiefs of Police has described visual confirmation "as one of the 'essential components' of training on ALPR use").

250. GIERLACK ET AL., *supra* note 4, at 59 (finding "[m]ost agencies require alert verification via mobile terminals or confirming calls to dispatch before officers act").

251. *Id.* at 15.

252. *Id.*; *see* Cyrus Farivar, *Due to License Plate Reader Error, Cop Approaches Innocent Man, Weapon in Hand*, ARS TECHNICA (Apr. 23, 2014, 3:40 PM), https://arstechnica.com/tech-policy/2014/04/due-to-license-plate-reader-error-cop-approaches-innocent-man-weapon-in-hand/ (finding that the driver of a BMW was stopped after the ALPR device "misread a '7' on [the driver's] license plate for a '2' . . . "alert[ing] the officers to a stolen Oldsmobile and not a BMW"); GIERLACK ET AL., *supra* note 4, at 15, 59 (finding "the systems' readers can have difficulty distinguishing between plates from different states" meaning ALPR "cameras might match a plate photo to a hotlist alert—but the plate may belong to a vehicle from the wrong state"); *see also supra* note 139 and accompanying text (discussing the risk of error associated with ALPR devices).

253. *See supra* notes 245–248 and accompanying text.

and/or plate color."[254] Stops such as the one in *Green* are felony stops—meaning officers face greater risks and are more likely to display their weapons.[255] In one instance where an individual was mistakenly stopped for being in possession of a stolen vehicle, the individual explained that the officer's gun was not pointed at him, "but it was definitely out of the holster."[256] The discretion officers have in deploying a weapon depends on the severity of the crime.[257] Therefore, it becomes increasingly important that ALPR devices are not misreading plates, especially as mistrust between law enforcement and minority communities continues to increase.[258]

States that have implemented similar provisions in their state laws can provide a guide to the federal statute as to what type of guidelines should be included to ensure accountability and that citizens are protected from misreads or inaccurate data.[259] New Hampshire and Montana's reasonable suspicion guideline should serve as the guide for implementing a system that strives to protect citizens from being pulled over based on inaccurate data.[260] Further, establishing these requirements in legislation clarifies the responsibilities of law enforcement officials, thus avoiding the problem in *Green* where the reasonable suspicion policies were unclear.[261]

254. ROBERTS & CASANOVA, *supra* note 4, at 14–15.

255. Farivar, *supra* note 252.

256. *Id.*

257. *Id.*

258. *See Race, Trust and Police Legitimacy*, NAT'L INST. OF JUST., (July 14, 2016), https://www.nij.gov/topics/law-enforcement/legitimacy/Pages/welcome.aspx (noting that "minorities are more likely than whites to view law enforcement with suspicion and distrust"); Hannah Fingerhut, *Deep Racial, Partisan Divisions in Americans' Views of Police Officers*, PEW RES. CTR., (Sept. 15, 2017), http://www.pewresearch.org/fact-tank/2017/09/15/deep-racial-partisan-divisions-in-americans-views-of-police-officers/ (finding that in a 2017 survey "whites give law enforcement warm ratings (74%)," whereas only 30% of black Americans gave a warm rating and 30% gave a "very cold rating"); Russell Heimlich, *Limited Black Confidence in Police*, PEW RES. CTR. (July 30, 2009), http://www.pewresearch.org/fact-tank/2009/07/30/limited-black-confidence-in-police/ (explaining that a 2007 survey found "about half (55%) of all African Americans express confidence in the police to do a good job enforcing the law, [and] just 38% are confident police will refrain from using excessive force on crime suspects and just 37% are confident that the police will treat all races equally"); *see also* notes 237–241 (explaining that in Oakland, the police department is more likely to deploy ALPR devices in black and Hispanic communities).

259. NEB. REV. STAT. § 60-3204 (2018) (requiring ALPR device systems be updated "at the beginning of each law enforcement shift if such updates are available"); *see also* N.C. GEN. STAT. §20-184(e)(noting law enforcement agencies shall update ALPR systems "every 24 hours if such updates are available or as soon as practicable after such updates become available").

260. N.H. REV. STAT. ANN. § 261:75-b(VIII) (2017); MONT. CODE ANN. § 46-5-118(1) (2017).

261. *See infra* notes 272–275.

3. Lower Cost Data Storage Increases Citizen Privacy Infringement

As the cost of data storage has drastically decreased, law enforcement agencies are now able to store a greater quantity of data for a substantially cheaper price.[262] However, tension exists between the desire to preserve data long-term in the hopes that it will prove useful in a later criminal investigation and the desire to protect citizen privacy rights.[263] Collecting data has enormous benefits for law enforcement; one such benefit is that it aids in criminal investigations.[264] The ACLU and other privacy advocates have criticized the law enforcement practice of mass aggregation of citizen data because private citizens are always leaving traces of themselves.[265] Analyzing that data allows police departments "to draw increasingly powerful inferences about [a] person's motives, desires, and behaviors."[266] In drafting legislation, Congress should focus on the aggregation of data because this is what links individuals to other instances where their plate information has been read, and it can paint a more vivid picture of the individual.[267]

In determining the appropriate length of time to keep collected data, the duration should not be any longer than necessary to accomplish the goals of the ALPR program.[268] One suggestion on a reasonable amount of time that data should be stored is three weeks.[269] Three weeks is effective because it is unlikely that law enforcement will be able to record an individual's license plate number multiple times across a three-week period, given the mobile nature of the devices.[270] Implementing limits on how long data can be stored is an appropriate way to allow law enforcement to continue carrying out their duties of protecting citizens while also ensuring the rights of citizens are not being violated.[271] New Hampshire has one of the shortest retention policies requiring deletion within three minutes if there is no match to a crime database, but this limitation is not as effective for law enforcement.[272] Such a short retention time restricts the capabilities of law

262. Rushin, *supra* note 151, at 20–21; Rushin, *supra* note 144, at 291–292.

263. Newell, *supra* note 180, at 398.

264. GIERLACK ET AL., *supra* note 4, at 13.

265. Steven D. Seybold, *Somebody's Watching Me: Civilian Oversight of Data-Collection Technologies*, 93 TEX. L. REV. 1029, 1035 (2015).

266. *Id.*

267. *See* Dryer & Stroud, *supra* note 19, at 264; *see also* Seybold, *supra* note 265, at 1035 (explaining that new developments in data storage allows more data to be stored and analyzed).

268. Dryer & Stroud, *supra* note 19, at 266–67.

269. Fisher, *supra* note 150, at 349.

270. *Id.*

271. *Id.*

272. N.H. REV. STAT. ANN. § 261:75-b(VIII) (2017).

enforcement to use these devices to solve crime.[273] Longer data retention policies, such as the three-year-period required in Colorado, opens up the potential for data to be mined—a concern of Justice Sotomayor in *Jones*.[274] As Justice Alito also noted in *Jones*, using GPS devices for long-term investigative monitoring "of most offenses impinges on expectations of privacy."[275] A three-week or so retention limit is already in effect in Maine and smaller police departments suggest this is not an unreasonable limit for data storage.[276] Therefore, three weeks achieves a balance between law enforcement needs and citizen privacy protections.[277]

However, a blanket prohibition of three weeks would be ineffective if law enforcement was relying on certain license plate numbers for an ongoing criminal investigation.[278] ALPR devices have played a crucial role in identifying individuals associated with a crime.[279] There should be exceptions in the legislation that allow law enforcement to keep the data for a longer period of time to learn more "about ongoing cases or to identify crime trends and patterns."[280] Several states have included in their statutes

273. Dryer & Stroud, *supra* note 19, at 228.

274. COLO. REV. STAT. ANN. § 24-72-113(2)(a) (2015); United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting)); YOU ARE BEING TRACKED, *supra* note 184, at 8 (highlighting that ALPR devices and the collected data "can be used for tracking people's movements for months or years on end").

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

276. ME. STAT. tit. 29-A, § 2117-A(5) (2009) (providing that data should be retained for twenty-one days); ROBERTS & CASANOVA, *supra* note 4, at 29 fig.14 (finding that Arlington, VA and Takoma Park, MD police departments limit data retention to 30 days); *id* at tbl.18 (noting that seven surveyed police departments had a data retention policy of less than 30 days whereas only five allow indefinite storage of data).

277. ROBERTS & CASANOVA, *supra* note 4, at 23 (finding one law enforcement community was able to able to use captured plate data to find vehicle scans of a missing elderly person allowing law enforcement to zone in on one narrow region to quickly locate a missing person who needed medical attention); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("[T]he government's unrestrained power to assemble data that reveal[s] private aspects of identity is susceptible to abuse.").

278. Fisher, *supra* note 150, at 349.

279. *See* Karen Farkas, *License-Plate Scanners Result in Few 'Hits,' but Are Invaluable in Solving Crimes, Police Say*, CLEVELAND.COM, https://www.cleveland.com/cuyahoga-county/2017/12/license_plate_readers_result_in_few_hits_but_are_invaluable_in_solving_crimes_police_say.html (last updated Dec. 5, 2017) (noting that ALPR devices aided in the arrest of a burglary suspect); Lisa J. Huriash, *License Plate Readers Are Solving Crime, Cities Say*, SOUTH FL. SUN SENTINEL (Jan. 22, 2016), https://www.sun-sentinel.com/local/broward/fl-coral-springs-license-plates-20160122-story.html (explaining that Miami-Dade police officers relied on a license plate reader alert to pull over a red Camaro that had been reported stolen and led officers to also discover a stolen gun in the vehicle).

280. GIERLACK ET AL., *supra* note 4, at 72; *see also* notes 67–68 and accompanying text (describing ways that the legislature could develop suggestions on how long law enforcement should keep license plate data).

methods of preserving data that is pertinent to a crime.[281] For example, Nebraska allows "captured plate data" to be stored longer if it is needed for "a warrant, subpoena, or court order."[282] These types of exceptions ensure that citizen data is not being stored and "mined for future intrusions into their daily behaviors," while also allowing law enforcement to carry out its duties effectively.[283]

4. Ensuring Benefits Continue to Outweigh the Harms Through Public Oversight and Auditing Systems

To ensure that ALPR devices are not being abused, it is necessary to include provisions that relate to public oversight and auditing systems.[284] However, it is also important to take steps to ensure that the policies are being followed.[285] To illustrate, the Boston Police Department accidentally released a substantial amount of unredacted license plate data.[286] This release demonstrated that the Boston Police Department was reckless in both their failure to follow their own guidelines and in their release of the data.[287]

In the case of the Boston Police Department, the fundamental problem was a lack of sufficient oversight.[288] The officers held on to the data for over six months, even though they were required to delete it after three months. [289] Additionally, the program was never audited to determine how well it was working or if the agency was following its own guidelines.[290]

---

281. CAL. VEH. CODE §2413(b) (West 2011) (allowing data to be stored longer than 60 days if "the data is being used as evidence or for all felonies being investigated"); MINN. STAT. § 13.824(2)(d) (2015) (prohibiting the use of ALPR devices from being used "to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant").

282. NEB. REV. STAT. § 60-3204(1)(c); *see also* COLO. REV. STAT. § 24-72-113(2)(a) (2015) (allowing "passive surveillance record[s]" to be stored for longer than three years if a claim has been filed or there is any other incident that may result in the record becoming evidence, then a preservation request can be made to preserve the data for a longer period); UTAH CODE ANN. § 41-6a-2004(1)(c)(i–iii) (2014) (allowing data to be preserved longer than the statutory limits if there is a "preservation request," "disclosure order," or if a state or federal warrant has been issued").

283. Fisher, *supra* note 150, at 349; ROBERTS & CASANOVA, *supra* note 4, at 14 (noting that arrests and recovery of stolen vehicles increases with the more ALPR devices that a community has implemented).

284. Dryer & Stroud, *supra* note 19, at 269–70.

285. Shawn Musgrave, *Boston Police Halt License Plate Scanning Program*, BOSTON GLOBE (Dec. 14, 2013), https://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-licence-plate-readers-amid-privacy-concerns/B2hy9UIzC7KzebnGyQ0JNM/story.html.

286. *Id.*

287. *Id.*

288. *Id.*

289. *Id.*

290. *Id.*

The Boston Police Department fiasco highlights the importance of oversight and the need for effective guidelines to ensure ALPR devices are used properly.[291] Ensuring that there is some system in place, whether it is in the form of audit requirements or oversight, can mitigate privacy concerns and hold law enforcement agencies accountable for their actions in relation to how ALPR devices are used.[292]

Civilian oversight would be an effective oversight method, rather than mere reliance on an internal police review board.[293] Civilian oversight promotes independence and transparency and can lead to systematic correction.[294] Additionally, this type of oversight, especially in the area of police departments, has been viewed as promoting "democratic principles" because it provides the public with a larger role in having control over their police departments.[295] Civilian oversight can be especially useful as law enforcement departments begin to implement ALPR technology and develop policies because it allows citizens to have a voice in the development of the police department practices, while also enabling the local community to have a method of connecting with the police department to discuss any inconsistences or flaws with the system.[296] However, of the country's top fifty police departments, only nineteen allow civilian review boards "to review and make recommendations related to departmental policies and practices."[297] The limited ability for civilian review boards to make recommendations regarding police department policies or practices has led to civilian-oversight boards being criticized as inefficient and ineffective.[298] Using civilian review boards to oversee data collection and retention policies of ALPR systems will require reconsideration of the powers granted to civilian review boards to ensure their recommendations have an impact.[299]

Police internal review boards pose more of a challenge for oversight because ALPR devices are implemented for public safety, so officers may be hesitant to follow oversight regulations that aim to protect citizen priva-

291. Dryer & Stroud, *supra* note 19, at 270.

292. INT'L ASS'N OF CHIEFS OF POLICE, *supra* note 215, at 48.

293. Seybold, *supra* note 265, at 1040, 1045.

294. *Id.* at 1046–47. *But see* Rachel Moran, *Ending the Internal Affairs Farce*, 64 BUFF. L. REV. 837, 869 (explaining that civilian review boards have been criticized as "'weak, ineffective, poorly led' and have had no measurable impact on police misconduct" (quoting Kami Chavis Simmons, *The Politics of Policing: Ensuring Stakeholder Collaboration in the Federal Reform of Local Law Enforcement Agencies*, 98 J. CRIM. L. & CRIMINOLOGY 489, 504 (2008))).

295. Udi Ofer, *Getting It Right: Building Effective Civilian Review Boards to Oversee Police*, 46 SETON HALL L. REV. 1033, 1039 (2016).

296. Seybold, *supra* note 265, at 1046.

297. Ofer, *supra* note 295, at 1041–43.

298. *Id.* at 1043–44.

299. *See generally id.* at 1044–51 (explaining that civilian review boards need to be tailored in ways that will effectively serve the community, such as ensuring that there is a means of public access for filing complaints and a way to ensure that the disciplinary actions are meaningful).

cy at the expense of promoting public safety.[300] Further, higher-ranking officers "may set a tone of disrespect and disregard for internal policies or may normalize improper behavior . . . as a 'cost of doing business.'"[301] Additionally, internal review boards tend to be biased towards police officers and present difficulties for citizens who are filing complaints about misconduct.[302] Filing a complaint can sometimes require burdensome and unnecessary requirements.[303] This is especially troublesome with ALPR data collection because the public might not be aware of how their community is using ALPR devices, making it more challenging for citizens to file a complaint.[304]

Another way of ensuring that ALPR devices are being used effectively is to implement an audit system so the public can gain an understanding of whether ALPR devices are effective.[305] Establishing reporting procedures and methods of oversight requires law enforcement agencies to make sure that all information obtained using ALPR devices is done in compliance with the statute.[306] Including an audit provision ensures accountability and that the devices continue to provide a benefit to the community.[307] ALPR devices should be monitored because they allow law enforcement to collect massive amounts of data at a level "we have never experienced."[308]

Police departments and other public entities using ALPR devices should also be required to submit statistical analyses or other reports that demonstrate the usefulness of ALPR devices.[309] The reports should include data on "the number of license plates scanned, the names of the lists against which captured plate data were checked, the number of hot list matches, the number of hot list matches that were incorrect, and the number of matches that resulted in arrest and prosecution."[310] Additionally, audit logs should

300. Seybold, *supra* note 265, at 1041–42.

301. *Id.* at 1041 (quoting Barbara E. Armacost, *Organizational Culture and Police Misconduct*, 72 GEO. WASH. L. REV. 453, 474–75 (2004)).

302. *Id.*; *see also* Moran, *supra* note 294, at 844 (noting that "[s]aying internal affairs units are the best means for protecting citizens from police misconduct is like saying foxes are the best guards for the henhouse—a notion even small children have found laughable").

303. Moran, *supra* note 294, at 855 (noting that the Cleveland Police Department "refus[es] to investigate unless the complainant both identified himself by name and signed the complaint" and that "the majority of Connecticut police departments refused to accept anonymous complaints, third-party complaints, or complaints from minors unaccompanied by a parent or guardian").

304. Seybold, *supra* note 265, at 1042.

305. Dryer & Stroud, *supra* note 19, at 269.

306. Fisher, *supra* note 150, at 346.

307. *Id.* at 349–50; *see also* ARK. CODE ANN. § 12-12-1805(a)(1–2) (2013) (requiring entities using ALPR systems to code statistical data into a format that can be accessible by the public for review).

308. Hubbard, *supra* note 10, at 21.

309. Fisher, *supra* note 150, at 349–50.

310. *Id.* at 349; *see also* CAL. VEH. CODE § 2413(e) (West 2011) (mandating reports to the California legislature each year); MD. CODE ANN., PUB. SAFETY § 3-509(e)(1–6) (Supp. 2018)

be maintained and checked to identify inconsistences that could signal the potential of abuse.[311] Audit logs can deter law enforcement from using the ALPR database inappropriately or for reasons unrelated to public safety if the officers are aware that their access to the data is being monitored.[312]

III. CONCLUSION

Automated license plate readers provide law enforcement with the tools to drastically increase their efficiency.[313] Current Fourth Amendment privacy jurisprudence cannot be effectively applied to ALPR devices in a way that balances law enforcement priorities with privacy interests.[314] With this increase in technological efficiency, lawmakers and regulatory authorities need to take steps to ensure that the public is not harmed with the increase in ALPR technology.[315] Congressional action can serve to clearly identify societal expectations of privacy, thus providing a guide to the courts as to how to analyze these ever-evolving technologies.[316] These proposed recommendations provide guidance on some of the most fundamental elements that should be included to ensure citizen privacy is protected but not at the expense of law enforcement.[317] ALPR devices are useful tools, but given their potential to acquire substantial amounts of private information regarding an individual's daily activities, it is of the utmost importance that Congress acts to protect citizen privacy.[318]

(requiring the Department of State Police and the Maryland Coordination and Analysis Center to report to the Senate Judicial Proceedings Committee and the House Judiciary Committee regarding the use of ALPR devices in the state each year).

311. INT'L ASS'N OF CHIEFS OF POLICE, *supra* note 215, at 48.

312. *Id.*; *see also* MINN. STAT. § 13.824(6)(b) (2015) (noting that "[t]he results of the audit are public . . . [and i]f the commissioner determines that there is a pattern of substantial noncompliance . . . by the law enforcement agency, the agency must immediately suspend operation of all automated license plate reader devices until the commissioner has authorized the agency to reinstate their use").

313. *See supra* Section II.A.

314. *See supra* Section I.A.

315. *See supra* Section II.B.

316. *See supra* Section II.B.2.

317. *See supra* Section II.C.

318. *See supra* Section II.C.