Vanderbilt Journal of Entertainment & Technology Law

Volume 24
Issue 4 *Summer 2022*

Article 3

2022

Big Brother is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces

Yash Dattani

Big Brother is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces

ABSTRACT

Automatic License Plate Readers (ALPRs) are an increasingly popular tool in police departments across the United States. At its core, ALPR technology functions in a relatively simple manner. The technology has two major components: the actual scanners, which record license plates, and the databases which collect, compile, and analyze this information for officers to access at the click of a button. Although this technology first came to the United States in 1998 as a form of rudimentary border security, its purpose and capabilities have rapidly grown. Now, in 2022, ALPR has evolved into a frighteningly powerful piece of technology, potentially capable of creating a system of mass government surveillance and chilling various constitutional protections. This Note acknowledges that this technology has bolstered the police's ability to fight crime, but argues that its use must be limited through appropriate judicial action and regulatory measures to protect the privacy of all US citizens.

This Note proposes the following reforms to address this issue: (1) a shift in the way the judiciary permits ALPR technology to be used by police; (2) new federal legislation to limit the aggregation and retention of this data; and (3) the creation of a federal agency to monitor ALPR databases. While some academics have proposed a new evidentiary standard within the judicial process and are creating federal legislation to better address the threats posed by ALPR, this Note's solution specifically ensures that this technology does not infringe on the constitutional rights of US citizens and the information collected is properly stored.

TABLE OF CONTENTS

On October 25, 2017, Eric J. Richard was driving his car when a Louisiana Police Trooper stopped him for reportedly following the car ahead of him too closely.[1] After Richard pulled over, the trooper asked him where he was coming from.[2] The trooper, however, already knew the answer to this question.[3] He knew that Richard had crossed the

1. *See* United States v. Richard, No. 2:18-CR-00355-01, 2019 WL 4011489, at *1 (W.D. La. July 24, 2019), *report and recommendation adopted*, No. 2:18-CR-00355-01, 2019 WL 4014325 (W.D. La. Aug. 23, 2019); *see also Louisiana Court Case Reveals Extensive Driver Tracking System,* THENEWSPAPER.COM (Sept. 5, 2019), https://www.thenewspaper.com/news/67/6786.asp [https://perma.cc/XV7J-QY4S] (summarizing the facts in *Richard*, 2019 WL 4011489).

2. *Richard*, 2019 WL 4011489, at *1.

3. *See id.*

border into Texas earlier in the day.[4] He also knew that Richard had recently entered back into Louisiana before the traffic stop.[5] The trooper knew this information before he even exited his squad car because he was able to quickly search Richard's license plate using Automatic License Plate Reader (ALPR) technology to track Richard's movements across state lines.[6] When Richard responded that he was simply coming from his job, the trooper viewed this as an "apparent lie" and extended the stop.[7] The trooper had no reason to track Richard prior to this stop, but because Richard's answer did not line up with the ALPR data, Richard was subjected to extensive questioning and was eventually arrested for a different crime altogether.[8] Richard's story is one of many, as more and more inhabitants of the United States are being subjected to police stops utilizing this highly invasive technology.[9]

ALPR scanners and the databases that compile data from the scans have become vital tools for US police forces.[10] While ALPR technology and the databases supporting them have been called a breakthrough because they provide officers the ability to identify vehicles associated with crimes, they also create significant privacy concerns, especially when considering the magnitude of data being collected and retained from US citizens' travels.[11] Although a viable tool for policing, modern ALPR poses a serious threat to Fourth Amendment privacy protections because of the intrusiveness of this technology. However, the industry is largely unregulated, and a lack of judicial clarity has furthered ambiguity over whether the use of this technology

---

4. *See id.*

5. *See id.*

6. *See id.*

7. *See Louisiana Court Case Reveals Extensive Driver Tracking System*, *supra* note 1.

8. *See id.*

9. *See, e.g.*, 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 225, 238 (2015) (discussing *United States v. Lurry*, 483 Fed. App'x 252 (6th Cir. 2012), a case in which the Defendant was stopped and subjected to an invasive search based on data collected by an ALPR).

10. *See* AXON AI & POLICING TECH. ETHICS BD., AUTOMATIC LICENSE PLATE READERS 5 (2019), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf [https://perma.cc/6V9C-2G4H]; Tom Simonite, *AI License Plate Readers Are Cheaper—So Drive Carefully*, WIRED (Jan. 27, 2020, 8:00 AM), https://www.wired.com/story/ai-license-plate-readers-cheaper-drive-carefully/ [https://perma.cc/N8HJ-BHQW] (describing how New York police forces have embraced plate reading technology).

11. *See Automatic License Plate Readers*, ACLU, https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers [https://perma.cc/E8UZ-TPJT] (last visited Dec. 14, 2021) (highlighting ACLU's concerns over the invasiveness of ALPR technology).

implicates constitutional protections.[12] Additionally, government and private sector investments have led to rapid advancement in ALPR scanners and databases, turning this once-remedial technology limited to border security into a powerful technology being rapidly implemented in police forces nationwide.[13]

In Richard's case, he challenged the constitutionality of the police's use of ALPR technology which led to his arrest, but the court chose to avoid the issue altogether.[14] Instead, the court held that the officer had reasonable suspicion to extend the traffic stop and arrest Richard on grounds separate from the ALPR search.[15] This case exemplifies a common trend in both state and federal courts of simply avoiding addressing the actual constitutionality of police use of ALPR in its modern form by ruling on alternative merits and issues entirely.[16]

This Note begins by describing the background and current state of ALPR technology and then explains why the courts' current approach to issues that arise from ALPR is ineffective.[17] Part II addresses the history of ALPRs, beginning with the technology's origin in the United Kingdom. Part III details relevant case law in federal and state courts that outline the current judicial approach to addressing ALPR. Part IV "analyzes the approach that courts currently use to analyze the Fourth Amendment issues which arise out of the use of ALPR technology by police." Finally, Part V proposes that the US Supreme Court directly address the rising privacy concerns over this technology.

12. *See id.* ("This information is often retained for years, or even indefinitely, with few or no restrictions to protect privacy rights.").

13. *See* Simonite, *supra* note 10.

14. *See* United States v. Richard, No. 2:18-CR-00355-01, 2019 WL 4011489, at *3 (W.D. La. July 24, 2019), *report and recommendation adopted*, No. 2:18-CR-00355-01, 2019 WL 4014325 (W.D. La. Aug. 23, 2019).

15. *See id.* at *3–4.

16. *See id.*

17. *See infra* Parts II–IV.

I. THE HISTORY OF ALPR TECHNOLOGY

A. The Origins of ALPR

In February 1974, a vehicle carrying soldiers and families in northern England was bombed by the Irish Republican Army (IRA).[18] Twelve people were killed instantly, and another fourteen were gravely injured.[19] In the following years, IRA bombs killed and wounded hundreds or more people in the United Kingdom, most often in London.[20] These events sparked the creation of the first form of ALPR technology.[21]

Because the bombs were frequently car bombs or otherwise brought into the city with vehicles, London's police force created a system that used closed-circuit television (CCTV) to monitor and record the license plates of vehicles entering and leaving major roadways.[22] The program was further developed under the "Project Laser" plan.[23] Police officers were able to utilize the information captured by CCTV to monitor license plates in order to identify and stop vehicles connected to the IRA terrorist attacks or other serious crimes.[24] The program was a great success, and the technology behind this system was coined Automatic Number-Plate Recognition (ANPR).[25]

In 1993, the ANPR system was incorporated into police forces all around London as part of the "Ring of Steel" camera network.[26] As a result, thousands of individuals connected to IRA bombings and other serious crimes were located and prosecuted.[27] Inevitably, ANPR's great

---

18. *Timeline—Worst IRA Bomb Attacks on Mainland Britain*, REUTERS, https://www.reuters.com/article/uk-britain-security-bombings-idUKTRE74F31Q20110516/ [https://perma.cc/D6KN-PKZK] (May 16, 2011, 6:49 AM).

19. *See id.*

20. *See id.*

21. *See History of ANPR*, ANPR INT'L, http://www.anpr-international.com/history-of-anpr/ [https://perma.cc/VYU5-DVLM] (last visited Oct. 24, 2021); *City of London's Ring of Steel Security*, CITY SEC. MAG. (July 18, 2018), https://citysecuritymagazine.com/police-partnerships/city-of-london-police-ring-of-steel/ [https://perma.cc/KZ9C-NMJN].

22. *See* KEITH GIERLACK, SHARA WILLIAMS, TOM LATOURRETTE, JAMES M. ANDERSON, LAUREN A. MAYER & JOHANNA ZMUD, LICENSE PLATE READERS FOR LAW ENFORCEMENT: OPPORTUNITIES AND OBSTACLES 7 (2014), https://www.rand.org/pubs/research_reports/RR467.html [https://perma.cc/JN6V-C6AH]; Lauren Fash, *Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy*, 78 MD. L. REV. ONLINE 63, 64 (2019).

23. *See* GIERLACK ET AL., *supra* note 22.

24. *See id.*

25. *See id.*

26. *See History of ANPR*, *supra* note 21.

27. *See* GIERLACK ET AL., *supra* note 22.

success in countering terrorism and combating general crime in London lead to other police forces outside of the city adopted the technology.[28] In 1997, the Police National ANPR Data Centre (NADC) was formed, allowing police officers to access and analyze all ANPR data captured in the United Kingdom irrespective of local police department territorial boundaries or counties lines.[29] The NADC centralized all police ANPR data collected by scanners in the United Kingdom, revolutionizing the way this data could be accessed.[30] The rapid development and success of this technology did not go unnoticed, and by 1998 the technology made its way across the Atlantic into North America.[31]

B. ALPR's Rise in the United States

In 1998, the United States Customs and Border Patrol (CBP) implemented this technology, similarly called ALPR, to increase border security.[32] ALPR showed great promise and was championed as an advancement of technology for US border security.[33] CBP used ALPR technology not only to monitor official entrances into the United States, but also remote portions of the border where vehicles commonly carry criminals with drugs, laundered money, or even victims of human trafficking.[34] After seeing the technology's initial success, CBP expanded the use of these scanners, implementing them as far inland as possible to combat border-related crime.[35] While the technology was originally intended solely for use at the border, the government soon found that its capabilities exceeded such a limited application.[36]

---

28. *See id.*

29. *See History of ANPR*, *supra* note 21.

30. *See id.*

31. *See Treasury and General Government Appropriations for Fiscal Year 1999: Hearing on S. 2312 Before the Subcomm. on Treasury & Gen. Gov't of the S. Comm. on Appropriations*, 105th Cong. 147 (1998) [hereinafter *Treasury and General Government Appropriations*] ("funding was provided in fiscal year 1998 for automatic license plate readers as part of the first phase of Land Border Automation initiative . . . ."); *see also* GIERLACK ET AL., *supra* note 22 (explaining how license plate readers were first used by the U.S. Border Patrol).

32. *See Treasury and General Government Appropriations*, *supra* note 31; GIERLACK ET AL., *supra* note 22.

33. *See* Fash, *supra* note 22, at 65 (discussing the success of ALPR in monitoring US borders).

34. *See* U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-049, PRIVACY IMPACT ASSESSMENT FOR CBP LICENSE PLATE READER TECHNOLOGY 5 (2017).

35. *See* Jay Stanley, *More Federal License Scanners Reported*, ACLU (June 21, 2012, 12:15 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/more-federal-license-scanners-reported [https://perma.cc/ERC8-WGVN].

36. *See* Fash, *supra* note 22, at 64–65.

Eventually, police departments caught on to the potential of this technology, and after initial investments by the Department of Homeland Security (DHS) and later investments by the private sector, ALPR technology rapidly grew in the United States.[37]

Today, ALPR technology scans thousands of vehicles without drivers' consent or knowledge.[38] Typically no bigger than a box of tissues with a single exposed lens, ALPR scanners can be easily mounted onto vehicles of any size.[39] These scanners are often hidden in plain sight and are discreetly mounted on not only police cars and emergency vehicles, but also tow trucks, traffic lights, and street poles.[40] The scanners are typically hardwired to power and are thus always on, actively capturing and recording data from all cars that pass through its view, regardless of whether or not there is an infraction taking place.[41] Both technological advancements and innovation in ALPR technology have driven down the costs of production and increased the capabilities of scanners in recent years.[42] Over the last decade, scanners have gone from simply capturing license plates to recording vehicles' make and model, noting distinguishable marks, and even detecting what is in the tow.[43]

C. Modern-Day ALPR Capabilities

As of 2022, an average ALPR scanner can scan and capture thousands of cars' license plates in only one minute, completely unbeknown to their owners.[44] Once captured, the data from each license

37. Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia,* 25 RICH. J.L. & TECH. 1, 4 (2019) (attributing rapid growth in ALPR to advancing technology and a "$50 million in grants to local police departments from the Department of Homeland Security").

38. *See id.* at 1.

39. *Id.*

40. *See id.* ("They can be mobile, attached to police vehicles and tow trucks, or stationary, posted on traffic lights or street poles. Although appearances vary, a typical ALPR is a rectangular box slightly smaller than a box of tissues with a circular lens visible on one end. When attached to the trunk of a vehicle, ALPRs appear in pairs pointing past the vehicle's tail lights.").

41. *See id.* at 2.

42. *See* Simonite, *supra* note 10 (commenting on how ALPR have become cheaper and widely accessible to police departments through investment in the private sector).

43. *See* Louise Matsakis, *Flock Safety Says Its License Plate Readers Reduce Crime. It's Not That Simple*, WIRED (Oct. 24, 2019, 12:00 PM), https://www.wired.com/story/flock-safety-license-plate-readers-crime/ [https://perma.cc/9VEQ-LZZ2] (noting that the Flock LPRs are capable of detecting people walking by, and whether they have a dog in tow).

44. *See* Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-

plate, which includes the date and time, is saved to a database.[45] These databases are both public and private, and several private companies actively boast about their extensive databases to incentivize police departments to contract with them.[46] While databases previously only provided rudimentary search capabilities, they have rapidly developed over recent years.[47] Today, several top databases, like Vigilant Solutions, flaunt not only a large number of high-quality scans produced by in-house scanners, but also several search and filter categories with powerful analytics which provide various levels of data and tracking services.[48] Further, license plates can now be searched against "hotlists" of plates compiled by law enforcement officials which have been previously associated with crimes.[49] To further incentivize police departments to use their services, some private ALPR companies rent or loan their advanced scanners to police departments.[50] This has allowed police departments with fewer resources to adopt this technology.[51] As offers like this spread, more and more officers across the nation are able to view drivers' location data at the click of a button.[52]

The potential impact of this technology (both positive and negative) cannot be understated. ALPR has been touted as a successful crime-stopping tool in police departments nationwide.[53] For example, in March 2019, Atlanta police accepted an offer from ALPR startup, Flock Safety, to install scanners in the Atlanta suburb, Zone 2, Beat 215.[54] The suburb was one of the city's most dangerous zones because of its disproportionately high crime rate.[55] Flock Safety provided the Atlanta police with thirteen solar-powered ALPR scanners and granted them

readers-legal-status-and-policy-recommendations [https://perma.cc/9THJ-JVE8] (describing the capabilities of ALPR scanners and databases).

45. *See id.*

46. *See id.*

47. *See id.*

48. *See id.*; *see also Bring Us Your Cases*, VIGILANT SOLS., http://www2.vigilantsolutions.com/bring-us-your-cases [https://perma.cc/3AQG-Y47L] (last visited Oct. 24, 2021) (providing details of Vigilant Solutions database capabilities).

49. *See* Jordan Steffen, *License Plate Readers Help Police and Border Patrol, but Worry Privacy Advocates*, L.A. TIMES (Dec. 26, 2010, 12:00 AM), https://www.latimes.com/archives/la-xpm-2010-dec-26-la-na-license-reader-20101226-story.html [https://perma.cc/AE6X-PH43] (explaining how "hot lists" function).

50. *See* Matsakis, *supra* note 43 (describing Flock Safety services which include renting ALPR scanners/cameras).

51. *See* Simonite, *supra* note 10.

52. *See* Matsakis, *supra* note 43.

53. *See id.*

54. *See id.*

55. *See id.*

full access to the Flock Safety database and accompanying analytic features free of charge.[56] The result was significant; Stuart VanHoozer, the county's deputy chief of police, said that six months after the ALPR scanners were installed, the reported number of robberies and nonresidential burglaries each dropped by 50 percent compared to the previous year.[57] Moreover, between March (when the scanners were first installed) and August, the area also saw less than half the number of "entering auto" crimes in comparison to the previous year.[58] Although VanHoozer declined to champion the Flock Safety scanners as the sole reason for the change in crime rates, he acknowledged that the police department saw "an incredible decrease in crime" after the ALPR scanners were installed.[59] Meanwhile, Flock Safety viewed the results as a large victory; today, Flock Safety's ALPR scanners are used in over 400 communities in thirty-five states.[60] Meanwhile, academic studies on the effect of ALPR have been largely inconclusive. While some have found that the readers do not deter crime, others have found that scanners specifically reduce certain types of crime or that the scanners result in the apprehension of a repeat offender at a quicker rate, thus reducing the prevalence of crime.[61]

Flock Safety is one of several private companies heavily invested in ALPR technology.[62] One of the most popular private databases that is routinely used by police is known as Vigilant Solutions.[63] Vigilant Solutions sells access to its massive database of more than five billion license plate scans collected across the country, accounting for over 1.5 billion reads to searches made by law enforcement agencies.[64] The database uses a global positioning system's (GPS) coordinates of wherever the vehicle queried was scanned or photographed to provide the searcher with a range of addresses.[65] While these databases boast about their role in impacting crime statistics, a majority of license plate scans are of innocent citizens' cars that happen to drive by Vigilant

56. *See id.*
57. *See id.*
58. *See id.*
59. *See id.*
60. *See id.*
61. *See id.*
62. *See id.*
63. *See id.*
64. *See Vigilant Solutions*, MOBILCOMM, https://www.mobilcomm.com/vigilant-solutions/ [https://perma.cc/ZR5X-NR3Q] (last visited Feb. 26, 2022); Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police for Deportations*, ACLU (Mar. 13, 2019, 11:00 AM), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data [https://perma.cc/C925-Q8VS].
65. *See* United States v. Yang, 958 F.3d 851, 853 (9th Cir. 2020).

Solutions' scanners.[66] A study by the Electronic Frontier Foundation highlighted this, reporting that of a sample size of 173 entities consisting of police departments, federal agencies, and sheriffs' offices in twenty-three states from 2016 to 2017, 99.5 percent of the approximately 2.5 billion license plates scanned belonged to cars whose owners were not involved in any crimes.[67] The impact of this technology cannot be understated, and as of 2022, there are several pressing issues regarding the police use of ALPR that must be addressed.

D. Pressing Issues with Police Use of ALPR in 2022

Recently, ALPR scanners have also produced dangerous situations as a result of their inaccuracies.[68] For example, in 2018, Brian Hofer and his brother were on their way home when the Oakland police pulled them over.[69] The officers immediately drew their weapons and ordered Hofer and his brother out of the car and onto their knees.[70] With guns drawn, the arresting officers detained both Brian and his brother.[71] The police pulled over the Hofers because a Vigilant Solutions ALPR scanner incorrectly flagged the Hofer's vehicle as stolen and pinged the police.[72] The Hofer's story is one of many that highlights the extent to which US inhabitants are tracked and monitored across the United States.[73] Moreover, the Hofer's experience also highlights a heavy reliance that US police forces place on ALPR data when conducting stops and arrests.[74]

The Northern California Regional Intelligence Center conducted research on the accuracy of ALPR data, finding that a concerning number of departments selected did not audit the accuracy of the data at all.[75] Of the data that could be found, it was estimated that the ALPR

66. *See* Brooks, *supra* note 37, at 6, 17.

67. *See* Tanvi Misra, *Who's Tracking Your License Plate?*, BLOOMBERG: CITYLAB (Dec. 6, 2018, 8:31 AM), https://www.bloomberg.com/news/articles/2018-12-06/why-privacy-advocates-fear-license-plate-readers [https://perma.cc/QUD4-GRU8].

68. *See* Charlie Warzel, *When License-Plate Surveillance Goes Horribly Wrong*, N.Y. TIMES (Apr. 23, 2019), https://www.nytimes.com/2019/04/23/opinion/when-license-plate-surveillance-goes-horribly-wrong.html [https://perma.cc/4B57-47PS].

69. *Id.*

70. *Id.*

71. *See id.*

72. *Id.*

73. *See id.*

74. *See id.*

75. *See* Lisa Fernandez*, Privacy Advocate Sues CoCo Sheriff's Deputies After License Plate Readers Target his Car Stolen*, KTVU FOX 2 (Feb. 19, 2019), https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen [https://perma.cc/C4HH-QAK4].

scanners led to mistakes about 10 percent of the time.[76] Despite this, most police departments turn a blind eye and instead focus on the positive effect ALPR usage has had on their ability to deter and prevent crime.[77]

Further, critics of ALPR implementation have reported that this technology is used in the United States to disproportionately surveil people of color.[78] For example, in 2015, police cars equipped with ALPR scanners targeted minority communities in Oakland, intentionally driving through lower-income areas to conduct multiple scans per day and collect more extensive data from these neighborhoods.[79] This data was used to aggressively surveil members of those communities to pretextually target them for potential offenses.[80] Lawsuits emerged against the same police departments after they granted the FBI unauthorized access to their ALPR scans, in violation of Oakland Privacy Advisory Commission policies.[81]

Presently, ALPR technology theoretically allows police departments to determine exactly where all US inhabitants are at any given time.[82] Depending on how robustly it has been implemented, the technology can develop detailed data about one's daily routine, place of work, and essentially all of one's travels.[83] Eighty-three percent of US adults drive a car several times a week.[84] These citizens are inevitably scanned in their locality by ALPR.[85] Data collected can be analyzed to reveal not only a person's trips to work or church, but also travel they assumed would remain private, such as numerous visits to a bar or doctor.[86] Police departments of all sizes invest in ALPR; 93 percent of

---

76. *See* Warzel, *supra* note 68.

77. *See id.*

78. *See* Annie Sciacca, *Oakland Police Give FBI "Unfettered Access" to License Plate Reader Data, According to Lawsuit*, E. BAY TIMES (Sept. 7, 2021, 6:30 AM), https://www.eastbaytimes.com/2021/09/04/oakland-police-give-fbi-unfettered-access-to-license-plate-reader-data-according-to-lawsuit/ [https://perma.cc/H4E5-TTVF].

79. *See id.*

80. *See id.*

81. *See id.* (discussing how providing the FBI "unfettered access" to the license plate data on the citizens of Oakland violated the city policy on sharing ALPR data outside the local police department).

82. *See* Zack Whittaker, *Police License Plate Readers Are Still Exposed on the Internet*, TECHCRUNCH (Jan. 22, 2019, 5:26 PM), https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/ [https://perma.cc/97K5-UKZQ].

83. *See* Jamela Debelak, *ALPR: The Surveillance Tool You've Probably Never Heard of*, ACLU WASH. (May 20, 2013), https://www.aclu-wa.org/blog/alpr-surveillance-tool-you-ve-probably-never-heard [https://perma.cc/N3X2-TLB9].

84. Díaz & Levinson-Waldman, *supra* note 44.

85. *See id.*

86. *See id.*

police departments in cities with populations above one million use ALPR, and 75 percent of police departments in cities with populations above one hundred thousand have implemented these systems.[87] These statistics clearly suggest that the police departments have an interest in the capabilities of ALPR technology.

Even though police departments in most states have implemented ALPR technology, there has been limited regulation of it.[88] As of January 2022, only a handful of states have passed ALPR-related regulations, and several others have considered and specifically declined to do so.[89] Of the states that have placed restrictions on the use of this technology, many have opted to carve out exceptions for common police functions.[90] For example, under the Utah Automatic License Plate Reader System Act, the use of ALPR is generally prohibited.[91] However, there are exceptions to the use of ALPR by law enforcement, specifically when police: (1) use the technology to protect public safety, (2) conduct criminal investigations, (3) comply with the law, (4) enforce parking laws, (5) enforce motor carrier laws, (6) collect a toll electronically, and (7) control access to a secured area.[92] Almost all activities undertaken by the police qualify for these exceptions.

Further, policies regarding how long such data can be stored and kept vary by state.[93] According to a report from the American Civil Liberties Union, the amount of times data is retained by a police department varies widely.[94] On the one hand, the Minnesota State Patrol deletes the data it collects after forty-eight hours.[95] On the other hand, New Jersey police departments are required to hold the data for

87. *Id.* (citing BRIAN A. REAVES, LOCAL POLICE DEPARTMENTS, 2013: EQUIPMENT AND TECHNOLOGY 4 (2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf [https://perma.cc/JL8M-69V4]).

88. *See* AXON AI & POLICING TECH. ETHICS BD., *supra* note 10, at 11 (noting the lack of regulation of ALPR technology in the United States despite its widespread implementation).

89. *See Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 3, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/6BBJ-RF8D]; Brooks, *supra* note 37, at 10.

90. *See* AXON AI & POLICING TECH. ETHICS BD., *supra* note 10, at 30.

91. *See* UTAH CODE ANN. § 41-6a-2003(1) (West 2022).

92. *See* § 41-6a-2003(2).

93. *See You Are Being Tracked*, ACLU, https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked [https://perma.cc/6V6F-K4TR] (last visited Dec. 13, 2021).

94. *See* ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 18, 20 (2013), https://www.aclu.org/sites/default/files/field_document/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/GNC5-2WN9].

95. *See id.* at 20.

over five years.[96] Additionally, some police agencies are allowed to use the information to assist and aid with criminal investigations nationally, while others are not.[97] The lack of uniform regulation of this technology is especially concerning because most police departments use ALPR.[98] State policies appear concerningly outdated and inadequate when considering how contemporary ALPR technology functions.

Despite the disparity in how the technology is regulated among the states, Congress has repeatedly refused to step in and regulate.[99] Congress's refusal is partly because any attempts at federal regulation have been met with fierce opposition by police lobbying groups.[100] Most notably, in 2015, the International Association of Chiefs of Police sent a peremptory letter to stop federal lawmakers, warning Congress of the adverse effects of future ALPR restrictions.[101] The letter vehemently stated the benefits of ALPR technology and expressed concerns over classifying ALPR as a national real-time tracking capability for law enforcement.[102] On the other hand, citizens have advocated for national regulation because of serious privacy concerns.[103]

Notwithstanding concerns that ALPR allows police departments to track US citizens, both Congress and the federal courts have largely avoided addressing the constitutionality of ALPR use.

---

96. *See id.*

97. *See id.* at 25–27.

98. *See id.* at 12, 20.

99. *See* Brooks, *supra* note 37, at 19.

100. *See* Cyrus Farivar, *Cops Are Freaked Out that Congress May Impose License Plate Reader Limits*, ARS TECHNICA (Mar. 15, 2015, 10:00 AM), https://arstechnica.com/tech-policy/2015/03/cops-are-freaked-out-that-congress-may-impose-license-plate-reader-limits/ [https://perma.cc/Z4AV-3FXY].

101. *See id.* ("[The International Association of Chiefs of Police is] deeply concerned about efforts to portray automated license plate recognition (ALPR) technology as a national real-time tracking capability for law enforcement. The fact is that this technology and the data it generates is not used to track people in real time. ALPR is used every day to generate investigative leads that help law enforcement solve murders, rapes, and serial property crimes, recover abducted children, detect drug and human trafficking rings, find stolen vehicles, apprehend violent criminal alien fugitives, and support terrorism investigations.").

102. *See id.*

103. *See id.* ("Mike Katz-Lacabe, a privacy activist in San Leandro, California, who famously shared photos that his city's police had taken of him and his daughters exiting their own car on their own driveway voiced his concerns against the technology. 'While it is technically correct that license plate readers do not track people in real time, it does track vehicles,' he wrote. 'Most of the time, that means you are tracking the person to whom the car is registered. It's the equivalent of stating that the stingray isn't used to track people, it's used to track a specific phone.'").

II. CONSTITUTIONAL ISSUES WITH THE POLICE USE OF ALPR

Over the years, several cases have examined the constitutionality of the police's use of advanced technologies like ALPR.[104] As of the publication of this Note, though, the Supreme Court has not required police officers to obtain a warrant to photograph license plates to compare against law enforcement databases.[105] Further, the Court has not required officers to meet a specific evidentiary standard to justify using this technology in the first place;[106] there are two reasons for this. First, due to the pervasive regulation of vehicles that travel on public highways, there is no expectation of privacy in the context of license plates.[107] Second, longstanding precedent holds that drivers on public roads cannot expect their movements to be kept private from the police.[108]

Over the years, as technological inventions were acknowledged as potential threats to individuals' Fourth Amendment rights, the Court began to recognize how "innovations in surveillance tools" can infringe one's right to privacy.[109] Most notably, in *Kyllo v. United States*, the Supreme Court held that police need a warrant to use thermal imaging to detect heat coming from a garage that would not be visible to a human eye to detect a marijuana production operation.[110] Although academics argue that certain First Amendment issues arise out of using ALPR,[111] this Note focuses on the Fourth Amendment issues posed by this technology.

A. Relevant Cases Addressed by the Supreme Court

The Fourth Amendment explicitly protects Americans from unreasonable searches and seizures.[112] The Supreme Court has expounded upon the text of the Fourth Amendment, positing that the purpose of the Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials."[113]

---

104. *See* Delaware v. Prouse, 440 U.S. 648, 662 (1979); Kyllo v. United States, 533 U.S. 27, 35–36 (2001).

105. *See Prouse*, 440 U.S. at 662.

106. *See id.* at 654–55.

107. *See* California v. Carney, 471 U.S. 386, 392 (1985).

108. *See* United States v. Knotts, 460 U.S. 276, 281 (1983).

109. *See* Carpenter v. United States, 138 S. Ct. 2206, 2208 (2018); *Kyllo*, 533 U.S. at 35.

110. *See Kyllo*, 533 U.S. at 40.

111. *See* Díaz & Levinson-Waldman, *supra* note 44.

112. *See* U.S. CONST. amend. IV.

113. Camara v. Mun. Ct. of San Francisco, 387 U.S. 523, 528 (1967).

A seminal case concerning the constitutionality of technology analogous to ALPR is *United States v. Jones*.[114] Although the case does not discuss ALPR technology, the Court considers a comparable level of intrusion by GPS technology.[115] In *Jones*, the police placed a GPS tracker on an individual's vehicle and then used the device to track that vehicle's movements on public streets.[116] The majority found that the conduct violated the Fourth Amendment, but not necessarily because of the information collected by the GPS tracker.[117] Instead, the Court held that the installation and monitoring of a GPS device without a warrant on an individual's vehicle was a trespassory search under common law.[118] The Court's approach has been coined the "trespass-based" rule.[119] The Court has historically held that where there is a physical trespass and intrusion, it likely triggers Fourth Amendment protection.[120] Regarding the Fourth Amendment issue, the Court concluded: "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[121] The Court refused to answer this question due to concerns over additional "thorny problems" that it wished to avoid at the time.[122]

In concurrence with the *Jones* majority, Justice Sotomayor addressed the issue of a reasonable expectation of privacy in one's public movements.[123] On the issue of an expectation of privacy to an aggregation of data of one's travels, Justice Sotomayor specifically notes that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[124] Justice Sotomayor highlighted the majority's refusal to address whether aggregation of one's public travel and movements impedes an individual's constitutional rights.[125] Such an answer would eliminate the constitutional limbo in which police use of ALPR resides.

---

114. *See* United States v. Jones, 565 U.S. 400, 412 (2012).
115. *See id.*
116. *See id.* at 402.
117. *See id.* at 413.
118. *See id.* at 409–11.
119. *See id.* at 421 (Sotomayor, J., concurring).
120. *See id.* at 409–11 (majority opinion).
121. *Id.* at 412.
122. *See id.*
123. *See id.* at 413–18 (Sotomayor, J., concurring).
124. *Id.* at 415.
125. *See id.*

Justice Alito, Ginsburg, Breyer, and Kagan joined the *Jones* concurrence, which urged the Court to consider this subject.[126] Specifically, Justice Alito encouraged the Court to focus on whether society is willing to recognize a reasonable expectation of privacy in the long-term monitoring of an individual's vehicle, rather than whether the government's installation of the GPS tracker constitutes a warrantless search.[127] The Justices criticized the majority for focusing on the trespass issue that "may have provided grounds in 1791 for a suit for trespass to chattels" rather than the actual privacy issue at hand—long-term monitoring of one's movements.[128] In the concurrence, the Justices highlighted the issues with a "trespass-based rule."[129] This rule establishes that when there is a "technical trespass" followed by evidence gathering, the Court will find the conduct to constitute a search, whereas, in circumstances without such a trespass, the Court finds that no search occurred.[130] The concurrence argued that the majority should have implemented the *Katz* test,[131] which places emphasis on whether a societal expectation of privacy was breached, instead of a trespass-based test, which focuses on whether a trespass occurred.[132]

In *Katz v. United States*, the Supreme Court clarified that the Fourth Amendment protects "people[,] not places," and established that Fourth Amendment protections apply when an individual has a subjective expectation of privacy which society finds objectively reasonable.[133] This test, however, did not replace the trespass-based test, which, as noted, has continued to be applied in subsequent cases.[134] Additionally, in *Jones,* the Supreme Court explicitly held that this reasonable expectation does not translate to publicly viewable information, like travel on public roadways, and the Court has never

126. *See id.* at 418–31 (Alito, J., concurring).

127. *See id.* at 418–19 ("Ironically, the Court has chosen to decide this case based on 18th-century tort law.").

128. *See id.*

129. *See id.* at 421–22 (explaining cases that highlighted caveats of the trespass rule).

130. *See id.* at 420–21.

131. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

132. *See id.*; *Jones*, 565 U.S. at 422 (Alito, J., concurring) ("[*Katz*] finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation.").

133. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

134. *See Jones*, 565 U.S. at 409–11 ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.").

held that aggregation of this information warrants constitutional protection.[135]

This gap between the lack of an expectation of privacy during travel on public roads in light of the acknowledged potential expectation of privacy on the aggregation of certain types of data on citizens is important because the *Katz* approach,[136] to implicate Fourth Amendment protections which limit the power of police to surveil citizens, moves the focus of the analysis from technical trespass, towards societal expectation of privacy. The *Katz* test,[137] however, has its own caveats. First, the test itself does not replace the trespass-based test despite being starkly different from the earlier trespass-based test. As a result, there is variety in the way in which courts across the nation address ALPR in the first place.

Moreover, the *Katz* test is also cumbersome to apply because it requires judges to consider a hypothetical reasonable person when evaluating a reasonable expectation of privacy.[138] This approach forces judges to consider both their own personal expectations of privacy and that of a hypothetical reasonable person in society, resulting in inconsistent rulings dependent on a specific judge's understanding of a cutting-edge technology.[139] Despite these issues, the concurrence held that while relatively short-term monitoring of a person's movements on public streets may be permissible, the government's tracking of the suspect for four weeks likely crossed the line.[140] This discussion is the closest the Supreme Court has come to addressing a reasonable expectation of privacy regarding the aggregation of data of one's movements.[141] Answering this question of whether ALPR technology potentially uses an aggregation of data of one's movements exceeding a societal expectation to privacy is key to determining the constitutionality of ALPR technology.

Another relevant Supreme Court case analyzing police use of twenty-first-century technology under the Fourth Amendment is *Carpenter v. United States*.[142] In that case, the defendant argued that the police's use of his historical cell phone data—specifically, his

135. *See id.* at 420, 424 (Alito, J., concurring) (noting the disharmony in the courts applying *Katz*).

136. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

137. *Id.*

138. *Id.*; *see Jones*, 565 U.S. at 427 (Alito, J., concurring).

139. *See Jones*, 565 U.S. at 427 (Alito, J., concurring).

140. *See id.* at 430.

141. *See id.*

142. Carpenter v. United States, 138 S. Ct. 2206, 2208–09 (2018).

location—violated the Fourth Amendment.[143] The Court found that such information, especially when viewed in the aggregate, allowed the police to track a person's routine and daily life.[144] These concerns, combined with the "depth, breadth, and comprehensive reach" of this data, as well as the "inescapable and automatic nature of its collection," implicated constitutional protections.[145] The Court in *Carpenter* alluded to several concerns raised today by citizens concerned about the lack of regulation on the police's ability to use ALPR technology, including concerns about the automatic nature of the data's collection and how driving—while voluntary—is necessary for a citizen to adequately participate in society.[146]

B. Relevant Cases Addressed by Lower Courts

Although the Supreme Court has not addressed how the police use of ALPR technology fares under the Fourth Amendment, lower courts have addressed this specific issue.

There are several recent cases which concern the constitutionality of unwarranted police use of ALPR databases. For instance, in May 2020, the United States Court of Appeals for the Ninth Circuit in *United States v. Yang* decided a case where the defendant challenged an ALPR database search under the Fourth Amendment.[147] In *Yang*, the police used ALPR technology to search through the Vigilant Solutions' database for the license plate of the defendant's vehicle to ascertain its location.[148] Vigilant Solutions provided the police with a timed scan of the defendant's vehicle and an address leading to the defendant's private gated residence.[149] After he was detained, the defendant argued that the ALPR technology used to track and locate him without a warrant violated the Fourth Amendment.[150]

---

143. *See id.* at 2212.

144. *See id.* at 2220.

145. *See id.* ("In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

146. *See id.* at 2218.

147. United States v. Yang, 958 F.3d 851, 853 (9th Cir. 2020).

148. *See id.*; *see also* MOTOROLA SOLS., DO MORE THAN JUST DETECT (2021), https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html?utm_source=vigilantsolutions.com&utm_medium=referral&utm_campaign=vigilantsolutions_redirect [https://perma.cc/7FJM-L2TY] (click "Download the Brochure") (overviewing the capabilities of Vigilant Solutions' ALPR technology).

149. *See Yang*, 958 F.3d at 853.

150. *See id.*

The majority's opinion highlights the difficulty posed by the ambiguous constitutionality of ALPR technology. Here, the court reasoned that, under *Katz*,[151] there was no reasonable expectation of privacy because Yang drove a rental car that was due back to a rental car company hours before the ALPR scanner located the vehicle at his residence.[152] Like the Supreme Court, the Ninth Circuit avoided addressing the constitutional implications of police use of ALPR technology. Instead, the court found that the rental car contract stated that the vehicle would be reported stolen if not returned by a specific time.[153] Accordingly, there was no reasonable expectation of privacy in the vehicle's location.[154]

Judge Bea's concurrence approached the issue differently.[155] Rather than focusing on whether the defendant had a reasonable expectation of privacy at the time, Judge Bea focused on the fact that only one ALPR scan was used to locate the defendant's vehicle.[156] This fact is important because Judge Bea highlighted how in this case, ALPR did not reveal an aggregation of the defendant's movements but rather a single location.[157] Judge Bea further opined that a single scan could not reasonably violate one's expectation of privacy, and hence no Fourth Amendment question was implicated.[158] This argument raises an interesting concern—ALPR technology functions off one or more scans: At what point does aggregation of these scans violate a societally recognized expectation of privacy? As of now, no court has answered this question.

As evidenced by current case law, the legality of police using ALPR technology is in limbo. Both Supreme Court and lower court rulings have failed to directly address ALPR technology and whether aggregation of one's public travels implicates Fourth Amendment rights. This Note next analyzes existing case law and suggests that judicial action clarifies the constitutionality of ALPR usage by the police.

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

152. *See Yang*, 958 F.3d at 861.

153. *See id.*

154. *See id.*

155. *See id.* at 862–63 (Bea, J., concurring).

156. *See id.*

157. *See id.* at 863.

158. *See id.* at 862.

III. THE CURRENT JUDICIAL APPROACHES TO CONSTITUTIONAL CONCERNS POSED BY ALPR ARE INADEQUATE

The current methods used to address the privacy implications posed by ALPR technology are inadequate. Under the Supreme Court's current doctrine, police use of ALPR in most situations does not constitute a search under the Fourth Amendment.[159] However, as more and more cases arise in the lower courts, the Court must eventually address this issue in more depth. The ALPR industry is rapidly growing.[160] As a greater number of police departments and companies invest in this technology, there is an increasing need for new judicial guidance. Specifically, courts must address whether police use of modern cutting-edge ALPR scanners and databases amounts to a constitutional "search."[161]

A. The Current Approach to Defining a Search Inadequately Addresses ALPR Technology

The Court's definition of a search under the Fourth Amendment is far from clear.[162] The Supreme Court first analyzed the constitutionality of certain police surveillance technologies in *Olmstead v. United States*.[163] In *Olmstead*, the trial court convicted the defendants for a conspiracy to sell illegal liquor in violation of the National Prohibition Act.[164] The conspiracy was discovered, however, because federal prohibition officers were spying on the defendants via wiretap, intercepting and recording months' worth of incriminating communications.[165] Notably, the officers tapped the wires "along the ordinary telephone wires" to ensure that there was no physical trespass on the defendants' properties.[166] As a result, the court that applied the trespass-based test found that there was no search because wiretapping public phone lines is distinct from a "real" physical intrusion.[167]

159. *See* Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 309–12 (2011).

160. *See Yang*, 958 F.3d at 853.

161. *See id.* at 853–54.

162. *See* Bradford P. Wilson, *Enforcing the Fourth Amendment: A Jurisprudential History*, 28 CATH. LAW. 174, 174–75 (1986).

163. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

164. *See id.* at 455.

165. *See id.* at 456–57.

166. *See id.* This was specifically done by the police to avoid concerns with the "trespass-based" test which placed a great emphasis on a physical trespass to constitute a search. *See id.*

167. *See id.* at 466.

Further, the court noted that tapping public phone lines on public property between the defendant's home was comparable to a police search on public property, like highways.[168] This holding confirms that the trespass-based test would not find police use of ALPR technology constitutes a search.[169]

On the other hand, the later-promulgated *Katz* test focuses on an individual's subjective privacy expectation in light of society's objective opinion of the reasonableness of that privacy expectation and the relative intrusiveness of the supposed privacy intrusion.[170] The Supreme Court has also drawn a sharp distinction between (a) primarily constitutional technology that improves the efficiency of legitimate policing, like certain digital tracking devices, and (b) unconstitutional technologies such as those in *Kyllo*, which give police an intrusive "extrasensory ability."[171] However, this framework gives a lot of deference to police departments that use various forms of modern technology, including ALPR.[172] Under this approach, the use of ALPR technology by police without a warrant likely fits comfortably under current constitutional doctrine.[173] This precedent highlights that a person does not have an objectively reasonable expectation of privacy when driving on public roads, which is precisely what ALPR captures.[174] Further, under this framework, the United States Court of Appeals for the Seventh Circuit in *United States v. Garcia* found that recording a person's movements in public is not especially intrusive, even when law enforcement uses advanced GPS surveillance to do so.[175] In the opinion, Judge Posner foreshadowed the dilemma posed by ALPR: "Should government someday decide 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."[176]

The rapid advancement and widespread implementation of ALPR technology is strikingly similar to Judge Posner's "program of

168. See *id.* at 465 ("The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.").

169. *See id.*

170. Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring).

171. *See* Rushin, *supra* note 159, at 305–09.

172. *See id.*

173. *See id.* at 309–12 (explaining that under both the *Katz* test and trespass-based test various forms of technology including ALPR are likely permissible).

174. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

175. *See* United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

176. *Id.* at 998.

mass surveillance of vehicular movements."[177] Today, ALPR scanners can survey millions of vehicles every second and record and collect data on vehicular movements through public and private databases, primarily for government use.[178] The unregulated use of this technology has led to racial profiling, pretextual searches, and overall stress on society's traditional expectations of privacy.[179] Despite this, the judiciary's applications of the *Katz* or trespass-based tests ultimately find that ALPR technology rarely constitutes a Fourth Amendment search.[180]

B. Current ALPR Usage Remains Unconstrained by Katz

As a result of the doubt cast by the Supreme Court as to whether a citizen has a subjectively or objectively reasonable expectation of privacy when traveling on public roads, ALPR does not constitute a search under current doctrine.[181] The Court has traditionally held that people have no reasonable expectation of privacy in public places, such as public roads and highways, because activities conducted in such places are easily viewable and visible to the public; thus, there is no reasonable expectation of privacy in those activities.[182] Considering this in light of the first part of the *Katz* test, it is unlikely that a court will find that citizens' privacy rights are violated when traveling on public roads.[183] Applying *Katz*, courts focus on whether the citizen exhibited a desire for or an expectation of privacy recognized by society.[184]

The second prong of the *Katz* test concerns whether or not the suspect's expectation of privacy would be recognized as objectively reasonable.[185] Historically, this prong is given greater significance than the first.[186] Although the definition of objectively reasonable is not specified in constitutional doctrine, there is a broader set of factors on how the Court determines this standard to give a narrower sense of what objectively reasonable entails.[187] In light of police activity, the

177. *See id.*

178. *See* Díaz & Levinson-Waldman, *supra* note 44.

179. *See* Sciacca, *supra* note 78.

180. *See* Rushin, *supra* note 159, at 309–313.

181. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

182. *See id.*

183. *See id.*

184. *See, e.g.*, Hudson v. Palmer, 468 U.S. 517, 525 (1983).

185. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

186. *See Hudson*, 468 U.S. at 525.

187. *See, e.g.*, United States v. Kim, 415 F. Supp. 1252, 1254–58 (D. Haw. 1976) (detailing the courts process in determining whether a new technology—telescopic photography—implicates a constitutional protection).

most important factors are: (1) whether the observation was made in plain sight, (2) the relative intrusiveness of the tactic, and (3) whether the police activity would have been offensive to the Framers of the Constitution.[188] In the context of ALPR, there is little question as to whether the observation could be made in plain sight because license plates are easily visible to passing bystanders. However, there is a significant level of intrusion when considering the relative invasiveness of ALPR technology, specifically the covert nature and the magnitude of information collected by ALPR technology.[189] The Court and academics state that this is likely outweighed by the fact that communities often elect to install ALPR scanners in their neighborhoods and contract with databases voluntarily.[190] This voluntary conduct indicates a value judgment made by the people within the areas subject to ALPR technology—specifically, that the value of this technology is greater than any potential privacy concerns.[191] The issue with such a conclusion is the lack of community participation in such decisions.[192] Several police departments choose to initially embrace this technology without community input, making the decision largely within the police department rather than within the community.[193]

Next, regarding whether the use of the technology would be conduct that the Framers would find offensive, an argument can be made that ALPR technology exceeds the bounds of anything the Framers could have conceived. Accordingly, attempting to consider whether the Framers would find the use of such technology "offensive" is unrealistic. Additionally, the difficulty in conceiving how the Framers would interpret cutting-edge technology only complicates matters.[194] Ultimately, it is up to the Supreme Court to determine what would offend the Framers. While judges cannot truly know what the Framers would consider offensive, they have construed that there is no legitimate, objectively reasonable expectation of privacy in one's

188. *See* Rushin, *supra* note 159, at 310–11.

189. *See* Díaz & Levinson-Waldman, *supra* note 44 (highlighting the magnitude of data collection of modern-day ALPR technology).

190. *See* Matsakis, *supra* note 43 (detailing how local officials and the police department choose to implement ALPR technology towards community safety interests); Rushin, *supra* note 159, at 315–16.

191. *See* Matsakis, *supra* note 43; Rushin, *supra* note 159, at 311.

192. *See* AXON AI & POLICING TECH. ETHICS BD., *supra* note 10, at 29 (discussing the importance of involving communities before law enforcement agencies adopt ALPR technology).

193. *See* Matsakis, *supra* note 43; Simonite, *supra* note 10.

194. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 567–76 (2017) (discussing how the Court has grappled with new and changing technologies for Fourth Amendment purposes).

activities on public roads, indicating the Court's belief that the Framers would not find ALPR technology offensive.[195]

In *United States v. Knotts*, the Supreme Court concluded that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[196] The Court specifically noted that when traveling down a public street, one voluntarily conveys to the public that he or she is traveling on a certain road, in a certain direction.[197] Further, the Court stated that by simply driving on a public road, a person knowingly conveys certain information to the public.[198] This information includes their general route, stops made during their travels, and even their final destination.[199] This holding suggests that if the Court were to consider the facts of *Yang*, it would hold that the defendant, by driving on public roads, was voluntarily conveying to all not only his current location but also the defendant's final destination, including the location of his private residence.[200]

Thus, considering the *Katz* test as it stands,[201] the Court would likely find that the police use of ALPR technology does not infringe on the defendant's Fourth Amendment rights.[202]

C. ALPR Technology Gives Law Enforcement a Significant Extrasensory Ability

In *Kyllo*, the Court placed great emphasis on the reality of law enforcement's sense-enhancing ability to intrude on one's privacy by using modern technology.[203] While ALPR technology does not necessarily give law enforcement an ability to intrude into the boundaries of the home, it does, in a way, give them extrasensory ability. That capacity, of course, is ALPR technologies capability of monitoring and tracking vehicles, unlike traditional police work.[204] While police may be able to follow a car or write down a plate number,

195. *See* Rakas v. Illinois, 439 U.S. 128, 152–53 (1978) (Powell, J., concurring); *see also* Rushin, *supra* note 159 (explaining that, under the Supreme Court's precedents, ALPR does not appear to violate the Fourth Amendment).

196. United States v. Knotts, 460 U.S. 276, 281 (1983).

197. *Id.* at 281–82.

198. *See id.*

199. *See id.* (highlighting how a "final destination" can include exiting a public road onto private property).

200. *See id.*; United States v. Yang, 958 F.3d, 851, 854–57 (9th Cir. 2020).

201. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

202. *See* Rushin, *supra* note 159.

203. *See* Kyllo v. United States, 533 U.S. 27, 34–35 (2001).

204. See Rushin, *supra* note 159, at 285–86.

such manual work is simply incomparable to how modern-day ALPR technology functions. Although the Court has placed great emphasis on the protection of an individual's home, there is merit in considering the strong extrasensory ability that modern-day ALPR technology gives to police, despite being used in the context of public roads.[205] Modern ALPR technology across the nation captures millions of license plates.[206] It can be used to track a vehicle and its driver across state lines and over days without any actual police officers physically acting.[207] Police use of ALPR, similar to the heat scanners in *Kyllo*,[208] very likely constitutes an extrasensory ability.

In *Dow Chemical Co. v. United States*, the Supreme Court held that technologies which substantially improve an officer's senses are constitutional.[209] There, the technology at issue was aerial photography, the use of which was without a warrant.[210] Although the aerial photography was detailed, it simply gave police the ability to get a bird's-eye view of a property.[211] Meanwhile, the officers still had to fly a plane with a camera mounted to it, and analyze the results.[212]

This technology is vastly different than ALPR technology, which is essentially always operating without any police interaction.[213] Other than the initial setup of sensors on vehicles or fixed areas, the sensors largely function without the aid of a police officer.[214] ALPR scanners capture potentially thousands of vehicles per second, and this data is automatically sent to ALPR databases that then compile and process it.[215] Although precedent suggests that it is not unconstitutional for police to use technology that substantially improves their sensory abilities, ALPR may have crossed the line into extrasensory.[216] It seems unlikely the Framers intended for the police to have unrestrained ability to implement invasive technologies on the premise that the technology does not infringe on the privacy of a home. There must be a

205. *See Kyllo*, 533 U.S. at 34–35.

206. *See* Díaz & Levinson-Waldman, *supra* note 44.

207. *See* Rushin, *supra* note 159, at 285–86.

208. *See Kyllo*, 533 U.S. at 34–35.

209. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

210. *See id.* at 229.

211. *See id.* at 238.

212. *See id.* at 229.

213. *See* Rushin, *supra* note 159, at 285–86.

214. *See id.*

215. *See id.*

216. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (discussing how the aggregation of data can present constitutional concerns). *But see* Rushin, *supra* note 159, at 309–13 (discussing how ALPR is likely constitutional under current doctrine).

line when it comes to police implementing technology to monitor citizen conduct, even if it occurs outside of the bounds of the home.

D. ALPR Databases Should Implicate Fourth Amendment Protections

In *Smith v. Maryland*, the Court held that warrantless access to pen registers (recording devices) used for telephone wiretaps does not raise Fourth Amendment concerns because a person should understand that their phone company keeps call records.[217] Therefore, because one knowingly and voluntarily turns over this information to the phone company, it is reasonable to expect the company to convey this information to others.[218] Consequently, telephone users do not have a reasonable expectation of privacy in their telephone records, notwithstanding the breadth of the information collected by the phone company.[219] This greatly differs from ALPR technology because drivers do not necessarily know of or understand the databases that compile and process ALPR data.[220] Rather, while drivers may understand that the details of their travels are conveyed to other citizens and police whom they drive past, they likely do not understand that they are knowingly conveying their license plate and location to several discrete ALPR scanners throughout their daily commute. ALPR technology concerns a part of life that many Americans simply cannot give up; a concept best illustrated in *Carpenter*—the use of a car is indispensable to the average citizen.[221] When someone drives their car, they do not consent to the use of ALPR technology; rather, it is used regardless of them giving their permission or not.

In *Smith*, the Court recognized the threat to privacy imposed by the accumulation of personal information.[222] The Court noted how collecting a single piece of data may not implicate the Fourth Amendment, but that the aggregation of such data could.[223] This directly relates to ALPR technology—while a single scan of a license plate likely does not implicate constitutional protections, at some point,

---

217. *See* Smith v. Maryland, 442 U.S. 735, 742–46 (1979).

218. *See id.* at 742–44.

219. *See id.*

220. *See* Brooks, *supra* note 37, at 1–3.

221. *Carpenter*, 138 S. Ct. at 2220 (discussing how cell phones and the services they provide are "such a pervasive and insistent part of daily life" that using one is essentially indispensable for participation in American society).

222. *See id.* at 2223.

223. *See id.*; *see also* Whalen v. Roe, 429 U.S. 589, 605 (1977) (noting the potential threat to privacy created by data accumulation and the mitigating role statutes, regulations, and the Constitution can play to address that threat).

the aggregation of numerous scans may.[224] Although the Court did not clarify at what point this threat implicates constitutional protections,[225] ALPR technology certainly appears to meet or exceed that threshold. These expansive databases not only store millions of scans generated each day, but also provide complex metrics such as live tracking and locational services.[226] Although the Court highlighted that every time a person gets in an automobile, one assumes the risk that law enforcement may document their movements,[227] this does not necessarily mean that one consents to being tracked by private ALPR database companies.

In short, the current approaches to address whether police use of advanced technologies implicates the Fourth Amendment are inadequate. Under the *Katz* test, courts cannot consistently address the concerns regarding police use of ALPR technology.[228] Additionally, under the older trespass-based test, courts cannot effectively analyze modern technologies like ALPR because it does not have a physical presence which constitutes a physical trespass.[229] However, by focusing on certain elements that have been recognized by the Court as significant (such as extrasensory ability),[230] it is conceivable to see how the use of this technology may implicate constitutional protections. All in all, the current approaches to addressing whether new technology implicates Fourth Amendment protections are outdated and in need of reform.

IV. PROPOSALS FOR BETTER REGULATING ALPR TECHNOLOGY

ALPR highlights the need for a legal shift in addressing the privacy implications of cutting-edge technology. Under the various current approaches, police departments can implement pervasive forms of surveillance in public areas and roads with disquieting ease.[231] There must be a transition in the judiciary's approaches that focuses not only on the capture or creation of a single piece of ALPR data, but also on the aggregation of these data points in databases. Although ALPR data

224. *See Whalen*, 429 U.S. at 605.

225. *See Carpenter*, 138 S. Ct. at 2223.

226. *See* Díaz & Levinson-Waldman, *supra* note 44; *see also Bring Us Your Cases, supra* note 48 (describing the features and services of Vigilant's ALPR databases).

227. *See* United States v. Knotts, 460 U.S. 276, 276 (1983).

228. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

229. *See id.* at 353 (majority opinion).

230. *See* Kyllo v. United States, 533 U.S. 27, 34–36 (2001).

231. *See* Warzel, *supra* note 68 (explaining how an ALPR database automatically prompted a dangerous police response without any supporting information).

captures something that a driver knowingly exposes to the public, the driver is not necessarily aware that the information is being aggregated, compiled, and analyzed. As a result, courts and lawmakers should limit ALPR in four ways. First, courts should rule that while ALPR technology itself is not necessarily unconstitutional, a search takes place when the information gathered from the aggregation of several "scans" exceeds what realistically could be achieved by physical police work. Second, the courts should rule that, in order to use ALPR in the first place, police forces must be able to demonstrate that an individual's actions satisfy the reasonable suspicion evidentiary standard. A lower evidentiary standard than probable cause, reasonable suspicion requires only that law enforcement demonstrate a particularized suspicion of criminal wrongdoing based on "specific and articulable facts" in conjunction with "rational inferences."[232] Imposing a minimum standard requirement on police access to ALPR data is necessary to reform the way police use this pervasive technology. Third, lawmakers should propose federal legislation which limits the amount of time ALPR scans and data can be retained. This legislation will better regulate ALPR technology and eliminate the different approaches followed by individual states. Finally, the government should create an agency to set standards, audit, and monitor the increasing number of private ALPR databases.

A. The Courts Should Implement a New Standard That Better Addresses When Cutting-Edge Technology Such as ALPR Can Be Used by Law Enforcement

The courts—especially the Supreme Court—are best positioned to address certain problems posed by ALPR. As of this Note's publication, all major privacy implications regarding pervasive technology and policing are primarily addressed by the courts.[233] ALPR poses great privacy implications, and the inadequacy of the courts' current approaches to ALPR and similar technologies warrants reform. The courts should not ban ALPR technology outright, but they should instead limit its use by police depending on the type of information

232. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968); *see also* Rushin, *supra* note 159, at 318 (explaining the evidentiary standard of "reasonable suspicion").

233. *See* Kade Crockford & Nathan Freed Wessler, *The Supreme Court's Big Privacy Ruling Sent a Message. Will Judges Hear It?*, ACLU, https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-big-privacy-ruling-sent-message-will-judges [https://perma.cc/QU2U-3KUK] (last visited Dec. 26, 2021) (highlighting the Supreme Court's power in dictating privacy protections for citizens from law enforcement).

being generated. To do so, the Court should implement a new standard to govern when and to what extent police can use ALPR.

The first and second proposals are important because they tie modern technologies, like ALPR, back to the physical ability of US police forces. This was a concept addressed by the Court in *Kyllo*, which found that police use of heat-ray technology to support the discovery of a marijuana plant operation was unconstitutional.[234] That holding was partially fueled by the fact that the heat rays in question were not actually physically visible to law enforcement on the scene.[235] As a result, the Court found that this sense-enhancing ability, in combination with the intrusion of one's home, warranted Fourth Amendment protections.[236] Similarly, the courts should find that if police evidence is generated by excessive and pervasive ALPR scans over an extended period of time, a search warrant should be required to access the information in question. Such an approach will drastically shift the way that current ALPR databases function.

These databases may have to change the way they operate, for example, by first notifying officers of the number of scans taken before allowing access to certain data. Alternatively, databases may instead display only the most recent scans before warning officers that accessing information over a longer period of time may constitute a search. This proposal follows the line of reasoning that the concurrence in *Jones* highlighted when they found that long-term civilian tracking constitutes a search in certain circumstances.[237] By warning officers that the use of certain features or live tracking capabilities may require a warrant, ALPR will be limited as a tool and can better reflect the physical capabilities of law enforcement. If the information sought is generated by a large aggregation of scans over an extended period, officers should instead pursue a search warrant to ensure that they are operating within the bounds of the Constitution.

This proposal also alludes to the privacy concerns mentioned in *Carpenter* regarding aggregating data.[238] Data that is by itself permissible when aggregated can be problematic and implicate constitutional protections. While calculating what law enforcement is physically capable of accomplishing will be difficult, this judicial

234. *See Kyllo*, 533 U.S. at 34–35.

235. *See id.*

236. *See id.*

237. It is important to note that the five justices in the majority opinion in *Jones* did not specifically find that long term tracking constitutes a search. *See* United States v. Jones, 565 U.S. 400, 424–25 (2012). While the justices considered that question, they stated that answering it would lead to "additional thorny problems" which they choose to avoid. *See id.* at 412.

238. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

approach will acknowledge that although police can employ cutting-edge technologies, they cannot circumvent constitutional protections. Further, as courts persistently implement this approach, the burden will be reduced as case law creates a clear precedent for courts to rely on in future decisions.

ALPR technology, at its core, functions as a two-part system. Data is first collected by scanning a vehicle traversing public roads or property, which is then compiled, analyzed, and processed through several complex and increasingly privatized databases.[239] As noted, there is little expectation of privacy when a single piece of ALPR data is scanned and collected because license plate numbers and locations can be observed at a certain point in time.[240] This is publicly viewable and not recognized as private information.[241] The concerns thus arise in the second part of this process, the aggregation of this data. These databases compile those single pieces of publicly viewable license plate information such as timestamps and vehicle make.[242] This data is then aggregated and manipulated to generate certain metrics depending on the number of scans within ALPR databases.[243] Such a system poses serious concerns because data generated by ALPR databases is treated equally regardless of whether it is produced by one scan or several scans over an extended period of time.[244]

Currently, some jurisdictions require that scans be deleted from all databases after a certain amount of time.[245] However, other jurisdictions do not place any limits on ALPR scan retention.[246] Considering that these databases and their content are available across state lines,[247] it is plausible that some scans are never completely deleted regardless of local policy. Therefore, it is important to place limits on this information's accessibility.

As it stands, ALPR technology potentially allows a police officer to survey and track citizens for any reason, whether it be pretextual

---

239. *See* Díaz & Levinson-Waldman, *supra* note 44.

240. *See id.*

241. *See id.*

242. *See id.*

243. *See id.*

244. *See id.*

245. *See, e.g.*, ME. REV. STAT. ANN. tit. 29-A, § 2117-A (2022); *see also* Dave Maas & Hayley Tsukayama, *EFF Joins Effort to Restrict Automated License Plate Readers in California*, ELEC. FRONTIER FOUND. (Mar. 19, 2021), https://www.eff.org/deeplinks/2021/01/eff-joins-effort-restrict-automated-license-plate-readers-california [https://perma.cc/QM6H-NX44] (discussing the push in California and other states for quick deletion of ALPR data from databases).

246. *See Automated License Plate Readers: State Statutes*, *supra* note 89 (listing the only sixteen states that have enacted ALPR limitations).

247. *See* Díaz & Levinson-Waldman, *supra* note 44.

(i.e., racial profiling) or genuine police work. To resolve this, courts should require that police officers (a) meet the evidentiary standard of reasonable suspicion to access single scans of ALPR data stored in a database, or (b) seek a warrant to access several scans of ALPR data compiled to provide locational and tracking services.

This proposal is important for several reasons. First, it immediately prevents this technology from being used in a racially motivated manner. As mentioned, ALPR technology has been disproportionately used in lower-income areas to target certain minority groups.[248] By requiring police officers to at least satisfy the reasonable suspicion standard before accessing the information stored in these databases, ALPR technology use in racially motivated ways will be significantly diminished. Further, by requiring that police officers obtain a warrant prior to receiving full access to tracking features and data compilations, officers will have to rely on traditional policing methods in addition to ALPR technology. This proposal will thus limit ALPR technology as a tool to fight specific crimes rather than allow it to operate as a generalized, expansive addition to US police surveillance capabilities.

This approach is in line with action taken by New Hampshire and Maine legislatures, both of which have implemented policies that require officers to have reasonable suspicion of a crime before using ALPR data to justify stopping an individual.[249] This limitation is important because it protects citizens from being subjected to police interactions solely based on ALPR data; it also requires that officers continue to depend on traditional law enforcement methods rather than information from private companies. By establishing an appropriate evidentiary standard, ALPR technology will remain a police tool rather than a crutch.

B. New Federal Legislation Should Be Enacted to Limit the Amount of Time ALPR Data Can Be Retained

There are also significant concerns over the lack of cohesion regarding the aggregation and retention of ALPR data, specifically due to the inconsistent state-by-state basis for standards regarding how long ALPR data can be stored and searched for.[250] This issue is two-pronged and can be adequately addressed by new legislation.

---

248. *See* Sciacca, *supra* note 78.

249. *See* N.H. REV. STAT. ANN. § 236:130 (2022); ME. REV. STAT. ANN. tit. 29-A, § 2117-A (2022).

250. *See Automated License Plate Readers: State Statutes*, *supra* note 89 (listing the varying laws of the only 16 states that have enacted ALPR limitations).

The way that ALPR data is currently retained depends on the state in which the police department resides: some states permit no data retention, some only permit retention on a specific criminal basis, and others permit retention for essentially an unlimited length of time.[251] This framework is problematic because state lines do not bind ALPR databases that collect this information.[252] Thus, to effectively limit this technology, there must be federal legislation which bars retaining information after a specified amount of time. Accordingly, lawmakers should pass federal legislation which bars retaining and storing ALPR scans gathered more than ten days prior, unless the data is flagged on a police hotlist. In the event the data is flagged on a hotlist because it is related to an active crime, it should be stored for a maximum of thirty days. An exception to this thirty-day requirement should be approved by a court on a case-by-case basis if law enforcement can demonstrate a compelling reason for an extension. Upon such a showing, it should be in the court's discretion to award additional time for data retention.

This restriction is vital to prevent ALPR technology from turning into a form of widespread police surveillance. Limiting the retention period of this data also ties ALPR scans closer to the realm of what is physically observable. Rather than giving officers the ability, especially in hindsight, to look at citizens' data collected months or even years ago, this policy would limit the amount of data aggregated and used in ALPR searches. Further, such a system balances the societal expectation of privacy with ALPR's crime-fighting capabilities.

Such a proposal is consistent with some states' current limitations on police surveillance technologies.[253] Maine, California, and New Hampshire have limited law enforcement surveillance, specifically ALPR, in several ways.[254] Maine has explicitly regulated ALPR technology by limiting how long police departments can retain scans to twenty-one days; it has also passed other reforms regarding confidentiality of the stored data.[255] In New Hampshire, the law limits all surveillance technology to specific investigations of crime and wrongdoing and bars long-term retention of this data in most situations.[256] Further, ALPR technology use by non-law enforcement

---

251. *Id.*

252. *See* Díaz & Levinson-Waldman, *supra* note 44.

253. *See Automated License Plate Readers: State Statutes supra* note 89.

254. *See id.* (listing the relevant ALPR statues for Maine, California, and New Hampshire).

255. ME. REV. STAT. ANN. tit. 29-A, § 2117-A (2022).

256. *See Automated License Plate Readers: State Statutes*, *supra* note 89.

officers or agencies is barred.[257] In California, the Senate Committee passed a bill in 2021 to limit ALPR data retention in order to block nationwide license plate tracking programs.[258] Previously, ALPR data in the state could be retained for sixty days unless it was being used as evidence or for the investigation of felonies.[259] The "investigation of felonies" exception results in the storage of ALPR data for years in several circumstances depending on the jurisdiction.[260] To prevent this, on March 23, 2021, the Senate Judiciary Committee of California passed SB-210, which restricts ALPR data significantly; the bill requires deleting and destroying collected data within twenty-four hours if it does not match a license-plate hotlist.[261] Additionally, the bill proposes annual audits to review ALPR search procedures and police conduct, and also requires detailed records of all police access to ALPR records.[262]

While these states have taken great steps in regulating ALPR, an issue still lingers. ALPR technology, especially in recent years, has become increasingly privatized.[263] The companies who run these databases are not bound within the confines of one set of state laws.[264] This makes it very difficult to determine whether data from a scan that is deleted or unavailable in one state is accessible by law enforcement in another. It also raises the concern of whether law enforcement can circumvent state restrictions by consulting with other police departments. Additionally, it is unclear if law enforcement agencies truly follow their governing states' regulations. For example, a 2019 audit of four local law enforcement agencies in California found that the agencies had accumulated large numbers of scans in their ALPR databases and were holding these scans for longer than necessary, even

257. *See id.*

258. Mike Maharrey, *California Senate Committee Passes Bill to Limit ALPR Data Retention, Help Block National License Plate Tracking Program*, TENTH AMENDMENT CTR. (Mar. 25, 2021), https://blog.tenthamendmentcenter.com/2021/03/california-senate-committee-passes-bill-to-limit-alpr-data-retention-help-block-national-license-plate-tracking-program/ [https://perma.cc/7RHM-Q4G7].

259. *See id.*

260. *See* CAL. VEH. CODE § 2413 (West 2022) (providing no limit on retention in the exception).

261. *See* Maas & Tsukayama, *supra* note 245.

262. *See id.*

263. *See* Brooks, *supra* note 37, at 11–13 (describing the rapid growth in the private sector of ALPR databases).

264. *See, e.g.*, Gil Aegerter, *License Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, NBC NEWS, https://www.nbcnews.com/news/world/license-plate-data-not-just-cops-private-companies-are-tracking-flna6C10684677 [https://perma.cc/ZMM4-KC26] (July 19, 2013, 3:44 AM) (listing companies operating in Illinois, Texas, Florida, and California).

though many were unrelated to criminal investigations.[265] There were also privacy concerns regarding the information's lack of protection, especially considering that two agencies were adding personal information to the scans, such as names, addresses, birthdates, and criminal charges of the vehicles' assumed drivers.[266] Further, in many circumstances, the agencies were sharing their scans and data with hundreds of other agencies without a clear explanation for doing so.[267] While ALPR regulation enforcement is beyond this Note's scope, this audit reveals the need for clear-cut policy when it comes to regulating ALPR nationwide.[268]

Federal legislation that would dictate the maximum amount of time that ALPR data can be stored is a first step in the right direction. This type of policy would address the concern of police departments in different states having access to certain scans as a result of differing local retention laws. Further, this legislation would uniformly regulate the use of this technology and balance the privacy interests of US citizens with the interests of US police forces. There is no doubt that ALPR technology is a powerful crime-fighting tool and that its use should not be banned outright, but regulations that limit when the technology can be used and how long the data it produces can be stored would ensure that it remains a tool rather than an unconstitutional mass surveillance system.

C. Congress Should Create a Federal Agency to Better Regulate ALPR Use by Law Enforcement and Other Actors

As ALPR technology has grown, law enforcement agencies have shifted from using government databases to private databases which boast impressive features, such as live tracking services and AI-powered metrics.[269] These private databases sometimes include a driver's personal information and license plate number.[270] As of this Note, numerous databases are competing to provide the best ALPR

265. *See* CAL. STATE AUDITOR, AUTOMATED LICENSE PLATE READERS 2 (2020), https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [https://perma.cc/S4ZV-KYVA].

266. *See id.* at 1.

267. *See id.* at 2.

268. *See generally id.* ("Law enforcement agencies must first create policies that set clear guidelines for how they will use ALPR data. Setting certain expectations in writing through an ALPR usage and privacy policy helps ensure that agencies operate their ALPR programs in a manner that better protects individuals' privacy.").

269. *See, e.g.*, PLATESMART, https://www.platesmart.com [https://perma.cc/TF8S-6SE3] (last visited Mar. 2, 2022).

270. *See* Díaz & Levinson-Waldman, *supra* note 44.

coverage across the nation by aggregating as many scans as possible.[271] The magnitude of this data cannot be understated, and the lack of clear-cut cybersecurity standards of this technology poses a threat to national security. This is detailed information being collected on essentially every US citizen that uses a motor vehicle. There must be government intervention that monitors and sets standards for all databases, both public and private, to abide by, especially considering the rising number of private databases emerging in this industry.

ALPR data has the potential to be used maliciously; thus, there must be immediate government intervention to safeguard this data. Therefore, Congress should establish a federal agency to ensure that databases follow strict data security standards and guarantee that the data is only accessible to appropriate officials. As the number of these databases grow, it is important that they abide by the best practices and privacy guidelines. There must be a government agency with clear standards to ensure that databases adequately protect this information. Additionally, having a federal agency audit and monitor databases is crucial to ensure that this data is appropriately stored and shared between authorized users (i.e., police departments). Further, because US police departments are highly decentralized, it is not uncommon for jurisdictions to share ALPR data amongst themselves.[272] These information transfers are done through various means, and it is important for them to be monitored so that sensitive information remains in the hands of properly authorized actors.

Lastly, the federal agency proposed by this Note can combat concerns of racial pretext raised by police use of ALPR. The proposed agency should implement audits and collect data to determine whether minority groups are disproportionately harmed as a result of the way the technology is being used. Additionally, the proposed agency should ensure that ALPR scanners are used uniformly across each police department's jurisdiction, rather than to target certain communities. There are rising concerns that ALPR technology is being rapidly implemented in minority communities to monitor and target these demographics.[273] Forming an agency that, at a minimum, monitors how police departments use ALPR technology will help address this issue.

There are two perspectives to address regarding racial pretext in police use of ALPR technology. On the one hand, ALPR advocates

271. *See*, *e.g.*, OPENALPR, https://www.openalpr.com [https://perma.cc/7SXZ-JR24] (last visited Mar. 9, 2022).

272. *See* Fash, *supra* note 22, at 87 (discussing why the decentralized nature of US police forces leads to potentially improper use of ALPR technology).

273. *See* Sciacca, *supra* note 78.

argue that this technology combats racial profiling in policing.[274] A report from Riverland Technology highlights how ALPR scanners are not influenced by subconscious bias or police officers' overt personal biases.[275] However, while the report focuses on how ALPR scanners are an automated technology—they function irrespective of police involvement—it does not properly acknowledge how ALPR searches themselves are still subject to racial bias.[276] As discussed, ALPR technology has been disproportionately and rapidly implemented by law enforcement in areas with high minority populations.[277] Although the technology itself may be unbiased because it is automated, the technology can be used to target minorities if law enforcement chooses to install a high number of scanners in certain areas. As it stands, this allows law enforcement to aggressively track minority populations.

V. CONCLUSION

ALPR poses a threat that the courts have long failed to fully address—the threat of a government system of mass surveillance.[278] Almost invisible to the naked eye, ALPR scanners across the nation scan and collect data on millions of Americans every day.[279] This data is then manipulated to track and locate targets.[280] The rapid development and implementation of ALPR technology have left it in a state which poses serious constitutional privacy concerns. As it stands, the current judicial approaches to governing the police use of this technology are inadequate. As a result, US police departments have been able to access and use this powerful technology with little constraint imposed.[281] While ALPR technology has great

274. *See Why LPR Eliminates Racial Profiling*, RIVERLAND-TECH, https://riverland-tech.com/alpr/why-lpr-eliminates-racial-profiling/ [https://perma.cc/7QDN-EHB9] (last visited Jan. 12, 2022).

275. *See id.*

276. *See* Sciacca, *supra* note 78.

277. *See id.*

278. *See* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

279. *See* Díaz & Levinson-Waldman, *supra* note 44.

280. *See id.*

281. *See id.*

crime-fighting potential, its use must be limited by the Fourth Amendment. Further, the information gathered by this technology must be effectively protected to prevent misuse. The solution to this problem requires courts and Congress to work together to implement a series of reforms. First, courts must establish standards which govern when police can use ALPR technology in the first place. These standards will ensure that ALPR remains a tool rather than a crutch in American police forces. Second, lawmakers must propose federal legislation to govern ALPR databases nationwide to (1) limit the retention of this data, and (2) set clear standards for the aggregation of this data. Finally, Congress should establish a government agency to ensure that ALPR databases are adequately protecting the large amounts of detailed information on US drivers they collect. Such an approach will protect the privacy interests of US citizens across the nation while allowing ALPR to continue to responsibly aid police in fighting crime.

*Yash Dattani**

* JD Candidate, Vanderbilt University Law School, 2022. The Author would like to thank Chandler Gerard-Reimer for her valuable insights and suggestions. The author would also like to thank his parents, partner and the editorial staff of the *Vanderbilt Journal of Entertainment and Technology Law* for their support and guidance.