DATA ON THE MOVE: THE INTERSECTION OF AUTOMATED LICENSE PLATE READERS AND PRIVACY IN INDIANA

ISABELLA PAGE*

INTRODUCTION

The implementation of Automated License Plate Readers ("ALPRs") across Indiana has experienced rapid growth, signifying a substantial increase in the reliance on ALPR technology by law enforcement agencies in the state.[1] Since 2022, the Indianapolis Metropolitan Police Department installed over 200 ALPRs, bringing the department's total to 321 readers.[2] This expansion shows no signs of slowing down, as the 2024 proposed budget plans for up to 150 additional readers throughout Indianapolis.[3] Many other communities in Indiana, such as Fishers, Muncie, Anderson, and Plainfield, also employ ALPRs.[4] In 2023, Gary, Indiana, received a $1 million federal grant for the purchase of additional ALPRs.[5] These cameras can potentially enhance law enforcement's investigative and crime prevention capabilities but also raise significant privacy concerns. [6]

ALPRs are a powerful tool that equips law enforcement with capabilities that would otherwise be virtually impossible.[7] The combination of cameras and computer software allows indiscriminate detection and storage of license plate numbers and other information of passing vehicles.[8] In addition to solving

---

* J.D. Candidate, 2025, Indiana University Robert H. McKinney School of Law; B.A. 2022, Indiana University – Bloomington, Indiana.

1. Anthony Schoettle, *Indiana Embracing License Plate Reading Devices*, IND. CHAMBER (June 8, 2022), https://www.indianachamber.com/indiana-embracing-license-plate-reading-device/ [https://perma.cc/YH5T-ZEDS].

2. Sarah Nelson, *Curbing Crime with Technology: 200+ License Plate Readers Coming to Indianapolis Streets*, INDIANAPOLIS STAR (Sept. 7, 2022, 12:26 PM), https://www.indystar.com/story/news/2022/09/07/200-license-plate-readers-coming-to-indianapolis-streets/65742787007/ [https://perma.cc/L6WH-X6XM]; David Gay, *IMPD Seeks to Expand Use of Technology to Improve Public Safety*, FOX59 (Sept. 13, 2023, 4:37 PM), https://fox59.com/indiana-news/impd-provides-update-on-use-of-crime-fighting-technology-in-department/ [https://perma.cc/J5JT-BX53].

3. David Gay, *IMPD Seeks to Expand Use of Technology to Improve Public Safety*, FOX59 (Sept. 13, 2023, 4:37 PM), https://fox59.com/indiana-news/impd-provides-update-on-use-of-crime-fighting-technology-in-department/ [https://perma.cc/J5JT-BX53].

4. Vic Ryckaert, *License Plate Readers Are Solving Crimes but Critics Fear Misuse, Privacy Concerns*, WRTV INDIANAPOLIS (July 25, 2023, 1:20 PM), https://www.wrtv.com/news/local-news/crime/license-plate-readers-are-solving-crimes-but-critics-fear-misuse-privacy-concerns [https://perma.cc/5N66-ALDS].

5. Lizzie Kaboski, *Gary Receives DOJ Grant for License Plate Readers*, THE TIMES (Aug. 12, 2023), https://www.nwitimes.com/news/local/crime-courts/gary-police-department-license-plate-readers-justice-grant-public-safety/article_dbd7d16e-38a7-11ee-9d89-b32fe4748a22.html [https://perma.cc/JR8Z-PVZG].

6. Ryckaert, *supra* note 4.

7. Ángel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations [https://perma.cc/MJZ4-LKVD].

8. *Id.*

crimes, ALPRs can be used to "investigate petty offenses, apprehend undocumented immigrants, generate fines and fees revenue, and track individuals over long periods of time."[9] The trail of data resulting from ALPRs allows law enforcement to view individuals' historical location information, which in turn can reveal sensitive details about someone's personal life.[10] There have been no state or federal constitutional challenges thus far with respect to the privacy implications of ALPRs; however, it is unlikely that Article 1, Section 11 of the Indiana Constitution or the Fourth Amendment of the United States Constitution provides sufficient protection.[11]

This Note argues that the best way to protect Hoosiers' individual privacy is by enacting legislation restricting the use, retention, and distribution of data collected by ALPRs. Part I of this Note explains how ALPR technology functions and the tradeoffs of its use. Part II then examines ALPRs under the Fourth Amendment, primarily relying on *Carpenter v. United States* to suggest that Fourth Amendment protection does not extend to encompass the privacy infringements arising from ALPRs, at least with respect to the current state of the technology.[12] Part III examines ALPRs under Article 1, Section 11 under the Indiana Constitution. Because of the lack of constitutional protection, Part IV argues it is incumbent on the Indiana Legislature to provide the necessary safeguards for their citizens and suggests model statutory language to accomplish this.

I. AUTOMATED LICENSE PLATE READER TECHNOLOGY

A. Capabilities

Indiana relies heavily on ALPR technology, as "[i]t's difficult to comb through Indiana police reports without stumbling across a mention of [ALPRs] these days."[13] An Indiana Assistant Police Chief praised ALPR's capability to identify license plates and search for the make, model or color of a vehicle; moreover, if queried for a "'person walking a dog, . . . it'll give you a picture of every person, and those are high-definition pictures and they work just as well

9. *Comprehensive Legislation on Automatic License Plate Readers: Overview*, POLICING PROJECT N.Y.U., https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/636f246df771a404c390bd3d/1668228205291/Legislative+Overview+ALPR.pdf [https://perma.cc/E3QV-EFNV] (last visited Nov. 26, 2023).

10. CATHERINE CRUMP ET AL., AM. CIV. LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 7-8 (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/V6FG-6V58].

11. *See generally* Litchfield v. State, 824 N.E.2d 356 (Ind. 2005).

12. Carpenter v. United States, 585 U.S. 296 (2017).

13. Schoettle, *supra* note 1.

at night as they do in the day.'"[14] Although there are various types of ALPRs, such as stationary or mobile cameras, their essential features are consistent.[15]

As the name suggests, ALPRs automatically photograph "all license plate numbers that come into view, along with the location, date, and time."[16] The captured data, which may include images of the vehicle and occasionally its driver and passengers, is then transmitted to a central server.[17] This enables law enforcement agencies to cross-reference plate numbers with "one or more databases of vehicles of interest."[18] Instead of mounting ALPRs on police vehicles as was done previously, Indiana has found it more effective to install them along roadways and attach them to traffic poles.[19] This placement provides for twenty-four-seven functionality, overcoming potential limitations such as officers having days off or their vehicles undergoing maintenance.[20]

ALPRs capture up to 1,800 license plates in a single minute at any time of the day.[21] Vigilant Solutions, an ALPR vendor Indiana is known to contract with,[22] offers stationary cameras with "infrared global shutter sensors that each scan at [thirty] frames per second," capturing clear images of vehicles moving up to 150 miles per hour, "even in zero lux conditions."[23] The cameras are designed for year-round use, as their lenses can scan as far as 125 feet away in

---

14. Steve Brown, *Police Access to Surveillance Cameras Concerns ACLU-Indiana*, FOX59 (Mar. 27, 2023, 5:43 PM), https://fox59.com/indiana-news/police-access-to-surveillance-cameras-concerns-aclu-indiana/ [https://perma.cc/ZRG7-HN8A].

15. *Street Level Surveillance: Automated License Plate Readers*, ELECTR. FRONTIER FOUND. (Oct. 1, 2023), https://www.eff.org/pages/automated-license-plate-readers-alpr#:~:text=ALPRs%20automatically%20capture%20all%20license,uploaded%20to%20a%20central%20server [perma.cc/3BUB-RMS4].

16. *Id.*

17. *Id.*

18. *Automated License Plate Recognition*, INT'L ASS'N OF CHIEFS OF POLICE, https://www.theiacp.org/projects/automated-license-plate-recognition [perma.cc/YGL9-B7TK] (last visited Nov. 26, 2023).

19. Casey Smith, *Data Privacy: What About License Plate Readers?*, IND. CAP. CHRON. (Feb. 1, 2023), https://www.heraldbulletin.com/news/state_news/data-privacy-what-about-license-plate-readers/article_986f6872-a25e-11ed-b9e7-1720d273f6cc.html#:~:text=Lawmakers%20have%20previously%20commended%20the,to%20follow%20the%20same%20rules [https://perma.cc/XP98-UDHH].

20. *Id.*

21. Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, THE ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ [https://perma.cc/4SYG-X3N5].

22. IND. INTEL. FUSION CTR., LICENSE PLATE READER POLICY 3 (2022), https://www.in.gov/iifc/files/Indiana-Intelligence-Fusion-Center-License-Plate-Reader-Privacy-Policy-2022.pdf [https://perma.cc/XN9S-6NDQ].

23. *L5F Fixed License Plate Recognition System*, MOTOROLA SOLS., https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/l5f-fixed-lpr-camera-system.html [perma.cc/YUT5-A7WR] (last visited Nov. 26, 2023).

rain, wind, or snow.[24] Even if cameras were purchased years ago, automatic software updates allow the devices to stay up-to-date.[25]

This initial "[d]ata collection is only the tip of the iceberg."[26] The camera systems are equipped with sophisticated software that enables creating and managing "hot lists and alerts, conducting detailed searches, and running patented, advanced analytics to reveal transformative vehicle location intelligence."[27] In Indiana, the oversight and administration of this software, provided by Vigilant Solutions, falls under the purview of the Indiana Intelligence Fusion Center Executive Director.[28] Their responsibility includes "ensur[ing] compliance with applicable laws, regulations, standards, and policy."[29] However, there are currently no specific Indiana or federal laws or regulations governing ALPR technology.[30]

B. Risks vs. Rewards

ALPR technology vendors emphasize the deterrent effects on crime, asserting that "as soon as cameras go up, police immediately solve more crimes . . . [a]nd then crime rates go down."[31] A 2018 controlled study found that police cars equipped with mobile ALPR technology demonstrated "a 140% greater ability to detect stolen cars" and identified up to four times more lost or stolen plates than cars without such technology.[32] This technology empowers the police "to be proactive with safety . . . [i]nstead of waiting for an incident to possibly occur, they will, in real-time, be alerted to any suspicious activity or persons that might present a safety issue."[33] To the extent ALPRs are used to prevent and solve crime, they can provide benefits to the community. However, the limited data available has led to widespread skepticism about the technology's actual effectiveness in reducing crime.[34]

While ALPRs earn praise for their crime prevention capabilities, they simultaneously evoke concerns about their impact on individual privacy. Single photos of license plates may not inherently raise alarms, but accumulating

---

24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. IND. INTEL. FUSION CTR., *supra* note 22.
29. *Id*.
30. *Id.*; *ALPR FAQs*, INT'L ASS'N OF CHIEFS OF POLICE (Aug. 8, 2018), https://www.theiacp.org/resources/alpr-faqs [https://perma.cc/9QH4-2FR4].
31. Schoettle, *supra* note 1.
32. Jason Potts, *Research in Brief: Assessing the Effectiveness of Automatic License Plate Readers*, POLICE CHIEF, Mar. 2018, at 14, https://theiacp.org/sites/default/files/2018-08/March%202018%20RIB.pdf [https://perma.cc/CEH3-E9FV].
33. Schoettle, *supra* note 1.
34. *Automated License Plate Readers: A Study in Failure*, INDEP. INST. (Nov. 30, 2021), https://www.independent.org/news/news_detail.asp?newsID=2294 [https://perma.cc/E832-7JPQ].

individual information in databases over prolonged periods warrants attention. The far-reaching capabilities of modern ALPR technology allow government agencies to transcend simple searches and hot list alerts, as the databases use powerful vehicle location analytics and possess billions of records.[35] Rather than capturing individuals' movements at a few locations, the vast amount of location data can result in a comprehensive view of individuals' daily movements, such as their places of worship, doctor's offices, educational institutions, residences, and more.[36]

In instances where police departments either lack policies or fail to enforce them rigorously, there is a heightened risk of technology abuse.[37] Just as cell phone data has been misused, ALPR data could easily be used to facilitate stalking.[38] Moreover, there are concerns about institutional abuse, as ALPRs allow law enforcement agencies to carry out systematic surveillance of political protestors, which has been seen in other nations employing this technology.[39] And generally, "[a]wareness that the government may be watching chills associational and expressive freedoms."[40]

With increases in the number of cameras, lengthy retention periods, and widespread sharing amongst agencies, law enforcement can assemble individual puzzle pieces to depict a high-resolution image of our individual lives.[41] The contribution of ALPR technology to police investigations should not be achieved at the cost of compromising individual privacy.

II. LACK OF CONSTITUTIONAL PROTECTION

A. Federal Fourth Amendment

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[42] Its purpose is to "safeguard the privacy and security of individuals

35. *L5F Fixed License Plate Recognition System*., *supra* note 23.

36. CRUMP ET AL., *supra* note 10, at 7.

37. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("The government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."); CRUMP ET AL, *supra* note 10, at 8; Marcus Green, *Kentucky and Indiana Police Are Collecting License Plate Data. Some Have No Policies for It*, WDRB.COM (Nov. 17, 2022), https://www.wdrb.com/wdrb-investigates/kentucky-and-indiana-police-are-collecting-license-plate-data-some-have-no-policies-for-it/article_6f637084-6692-11ed-9e9b-df1c220fe9b9.html [perma.cc/C7XS-7QES].

38. CRUMP ET AL, *supra* note 10, at 9.

39. For example, in the United Kingdom, an individual was pulled over based on an ALPR hit after his license plate was put on a hot list after an anti-war protest. *Id.*

40. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

41. CRUMP ET AL, *supra* note 10.

42. U.S. CONST. amend. IV.

against arbitrary invasions by government officials."[43] Accordingly, "when an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,'" intrusion into that private sphere generally qualifies as a search and requires a warrant.[44] Thus, a two-part test has emerged: (1) whether the subject of the search has an expectation of privacy, and, if so, (2) whether that subjective expectation is reasonable, judged by the objective criterion of the views of society as a whole.[45]

Whether an expectation of privacy is objectively reasonable is "informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'"[46] The Supreme Court has recognized two corresponding "guideposts" to inform the Court's analysis: (1) "seek[] to secure 'the privacies of life' against 'arbitrary power'"; and (2) "place obstacles in the way of a too permeating police surveillance."[47] However, when an "intrusion serves special government needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the [g]overnment's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[48] Still, "[e]ven where it is reasonable to dispense with the warrant requirement in the particular circumstances, a search ordinarily must be based on probable cause."[49]

1. Defining the "Search."—The single capture of a license plate is not the cause of concern but rather the sensitive information that can potentially be revealed from the accumulated data when assembled and compared to other relevant information. Without restrictions, ALPR data can be retained for years, and when compiled, it reveals much more detailed information than in isolation.[50] With this in mind, it is important to specify that the "search" does not occur when the ALPR captures a single photo of a license plate or from the passive accumulation of data within the database.[51] Rather, the search arguably occurs when law enforcement accesses and subsequently assembles vast amounts of historical data in a way that reveals personal information about an

43. Carpenter v. United States, 585 U.S. 296, 303 (2018) (quoting Camara v. Mun. Ct. of City & Cnty. Of S.F., 387 U.S. 523, 528 (1967)).

44. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

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

46. *Carpenter*, 585 U.S. at 304-05 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

47. *Carpenter*, 585 U.S. at 304-05 (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

48. Nat'l Treasure Emps. Union v. Von Raab, 489 U.S. 665-66 (1989).

49. *Id.* at 667.

50. CRUMP ET AL., *supra* note 10.

51. *See* Peterson v. State, 674 N.E.2d 528, 535 (Ind. 1996) (recognizing a search connotes prying into hidden places); United States v. Brown, No. 19 CR 949, 2021 WL 4963602, at *3 (N.D. Ill. Oct. 26, 2021) (citing United States v. Miranda-Sotolongo, 827 F.3d 663, 667-68 (7th Cir. 2016)) (finding no privacy interest in license plates).

individual that is otherwise not available to the naked eye.[52] This concept parallels the mosaic theory, which asserts that the "government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic."[53]

The mosaic theory first emerged when the D.C. Circuit Court ruled that the government's warrantless installation of a GPS device on a defendant's car and subsequent tracking of the defendant for twenty-eight days was an unreasonable search.[54] Invoking the mosaic theory, the Court held that "the whole of a person's movement over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[55] However, when the Supreme Court affirmed the D.C. Circuit Court on the merits in *United States v. Jones*, it did so under a narrower trespass of property rights theory.[56] Nonetheless, an argument for ALPR privacy violation emerges from the majority's acknowledgment that 4-week electronic surveillance "*without an accompanying trespass* [could result in] an unconstitutional invasion of privacy."[57]

The concurrences in *Jones* more closely echo the mosaic theory and are applicable to ALPR technology.[58] Justice Sotomayor explained how "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[59] And the fact that "GPS monitoring is cheap" and "proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[60] Also relevant to license plates, Justice Sotomayor opined that simply because an individual discloses information voluntarily to the public for a limited purpose does not disentitle that information to Fourth Amendment protection.[61] Justice Alito suggested that length of time matters because although "short-term monitoring of a person's

---

52. *See* CRUMP ET AL, *supra* note 10, at 9 (explaining that this assembly might often occur with reference to other sets of data or information. For example, if data is shared across various agencies, more detailed information will be revealed. Also, if the location points are mapped out against identified buildings, law enforcement could reasonably infer where someone frequents.).

53. United States v. Tuggle, 4 F.4th 505, 517 (7th Cir. 2021) (quoting Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205 (2015)).

54. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).

55. *Id.* at 560.

56. United States v. Jones, 565 U.S. 400, 404 (2012) ("Government physically occupied private property for the purpose of obtaining information.").

57. *Id.* at 412 (emphasis added).

58. *Id.* at 413-31 (Sotomayor, J., concurring) (Alito, J., concurring).

59. *Id.* at 415 (Sotomayor, J., concurring) (citing People v. Weaver, 12 N.Y.3d 433, 441-42 (2009)).

60. *Id.* 415-16 (Sotomayor, J., concurring) (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

61. *Id.* at 418 (Sotomayor, J., concurring).

movements on public streets accords with [society's reasonable] expectations of privacy, . . . longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[62]

Shortly after *Jones*, the Supreme Court endorsed the mosaic theory in *Riley v. California* by ruling that a warrantless search of cell phone contents was unconstitutional.[63] The court noted that a "cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record . . . [and] data on the phone can date back for years."[64] The Supreme Court acknowledged there will be "some impact on the ability of law enforcement to combat crime. But the Court's holding is not that the information on a cell phone is immune from a search; it is that a warrant is generally required before a search."[65]

Furthermore, the Supreme Court in *Carpenter v. United States*[66] effectively endorsed the mosaic theory when it held the government's collection of a defendant's cell-site location information for 127 days amounted to a search.[67] The location information provided an "all-encompassing record" which uncovered "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[68] *Carpenter* ultimately delineated the difference between short-term tracking of public movements and "prolonged tracking that can reveal intimate details through habits and patterns"; the latter form of surveillance invades expectations of privacy in the whole of a person's movements and therefore requires a warrant.[69]

Given that license plate numbers are intended to furnish information to law enforcement and are always visible to the public, the mere act of capturing a photo or maintaining a record of license plate numbers is unlikely to be deemed a search. Nevertheless, a compelling Fourth Amendment challenge to ALPRs emerges within the framework of the mosaic theory. Still, the tracking must reach a level of pervasiveness that effectively "paint[s] the type of exhaustive picture of [someone's] every movement that the Supreme Court has frowned upon."[70] Additionally, while the Supreme Court has implicitly endorsed the

---

62. *Id.* at 430 (Alito, J., concurring) (citing United States v. Knotts, 460 U.S. 276, 281-82 (1983)).

63. Riley v. California, 573 U.S. 373 (2014).

64. *Id.* at 375.

65. *Id.* at 376.

66. *See* discussion of *Carpenter* applied to ALPRS *infra* Sections II.A.2.

67. Carpenter v. United States, 585 U.S. 296, 316 (2018); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 373 (2019).

68. *Carpenter*, 585 U.S. at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

69. *Carpenter*, 585 U.S. at 296; Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021).

70. United States v. Tuggle, 4 F.4th 505, 524 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022) (reasoning that stationary cameras around the defendant's home captured an important sliver of his life but were not exhaustive enough to be unreasonable).

mosaic theory in several cases,[71] it has "not received the Court's full and affirmative adoption," and thus, lower courts are not bound to apply it when assessing a Fourth Amendment challenge.[72]

2. An Expanded Analysis of Carpenter v. United States and ALPRs.—In *Carpenter*, the Supreme Court ruled the government's warrantless acquisition of cell-site location data via a third-party company violated the Fourth Amendment.[73] In this case, law enforcement "obtained 12,898 location points cataloging [Defendant's] movements [over 127 days]—an average of 101 data points per day."[74] The Supreme Court held that the "detailed, encyclopedic, and effortlessly compiled" data violated an individual's "legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information] (CSLI)," whether the surveillance is employed by the government or by a third party.[75] The Court further noted that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[76]

Like the CSLI data, the location records resulting from ALPRs have the potential to "hold for many Americans the 'privacies of life.'"[77] ALPR databases similarly possess a "retrospective quality," providing law enforcement with access to "information otherwise unknowable."[78] And "[c]ritically, because the location information is continually logged for [every person that passes by]—not just those [] who might happen to come under investigation—this newfound tracking capacity runs against everyone."[79] In *Carpenter*, there is some contention regarding the precision of cell-tower location data—specifically whether it is as precise as GPS data or only provides a general location.[80] With ALPRs, there is no question that the technology possesses GPS-level precision, regardless of whether the reader is fixed or mobile.[81] Further, a person should not be deemed to "voluntarily 'assume[] the risk' of turning over a

---

71. *See Carpenter*, 585 U.S. at 296; *Jones*, 565 U.S. at 400 (2012) (Sotomayor, J., concurring) (Alito, J., concurring); Riley v. California, 573 U.S. 373 (2014).

72. *Tuggle*, 4 F.4th at 517, 519-20.

73. *Carpenter*, 585 U.S. at 310 (2018).

74. *Id.* at 302.

75. *Id.* at 309-10 (comparing to GPS monitoring considered in *Jones*, 565 U.S. 400 (2012)).

76. *Id.* at 310 (citing Katz v. United States, 389 U.S. 347, 351 (1967) ("What [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.")); *see also Jones*, 565 U.S. at 430 (individuals have a reasonable expectation of privacy in the whole of their movements).

77. *Carpenter*, 585 U.S. at 311 (quoting Riley v. California, 573 U.S. 373, 403 (2014)); *see also* CRUMP ET AL., *supra* note 10.

78. *Carpenter*, 585 U.S. at 312 (2018).

79. *Id.* ("Police need not even know in advance whether they want to follow a particular individual, or when.").

80. *Id.* at 313.

81. *L5M Mobile LPR Camera System*, MOTOROLA SOLS., https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/l5m-mobile-lpr-camera-system.html [https://perma.cc/J3V5-3TSR] (last visited Nov. 25, 2023).

comprehensive dossier of his physical movements" merely by driving a car.[82] A license plate is logged by ALPRs by "dint of its operation, without any affirmative act" beyond driving down the road.[83]

Although ALPR *capabilities* are comparable to CSLI data, the current *reality* of ALPR implementation likely does not warrant Fourth Amendment protection.[84] Where the CSLI data provided an "all-encompassing record of the holder's whereabouts," ALPRs are less prevalent than cell towers.[85] Rather than being "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years,"[86] there are gaps in a person's movements due to the limited number of cameras actually installed, even though the surveillance is activated twenty-four-seven. While the government can access a "deep repository of historical location information" with "just the click of a button," the depth of data on a particular individual is limited.[87]

Additionally, there is some suggestion in *Carpenter* that no matter how many ALPRs are implemented, the technology may never invoke Fourth Amendment protection:

> While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. . . . Accordingly, when the [g]overnment tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.[88]

Thus, it seems that because license plates only follow their owners on public thoroughfares, the government cannot achieve perfect surveillance like it can with cell phone data.

However, "the Court has already rejected the proposition that 'inference insulates a search.'"[89] Although license plates do not follow their owners indoors, with enough license plate readers, law enforcement could often infer which buildings someone entered and exited without knowing what they did while inside.[90] Accordingly, if ALPRs were situated sufficiently, the government could, in combination with other information and with the ability

82. *Carpenter*, 585 U.S. at 315 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

83. *Id.*

84. *See* Kyllo v. United States, 533 U.S. 27, 36 (2001) ("Must take account of more sophisticated systems that are already in use or in development"); *Carpenter*, 585 U.S. at 313 ("While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision.").

85. *Carpenter*, 585 U.S. at 311.

86. *Id.* at 315.

87. *Id.* at 311.

88. *Id.* at 311-12 (citing Riley v. California, 573 U.S. 373, 403 (2014)).

89. *Id.* at 312 (quoting *Kyllo*, 533 U.S. at 36).

90. Diaz & Levinson-Waldman, *supra* note 7.

to cross-reference the plate with other systems, "deduce a detailed log of [an individual's] movements."[91]

3. Post-Carpenter and ALPR Challenges.—Nevertheless, post-*Carpenter* Fourth Amendment challenges to ALPRs align with *Carpenter's* suggestion that ALPRs are not pervasive enough. Although the Supreme Court has yet to address the Fourth Amendment implications associated with ALPRs specifically, several district courts have asserted that ALPR usage does not constitute an unreasonable search. For instance, in *United States v. Brown*, the Illinois District Court found no privacy violation because law enforcement "did not obtain the 'privacies' of [the defendant's] life or exploit a too permeating police surveillance."[92] The ALPR found the car on public streets twenty-three times in a little over two months, and the court reasoned this was "the product of routine, non-invasive surveillance and did not upset settled expectations of privacy."[93]

Similarly, in *United States v. Bowers*, the Pennsylvania District Court held the government's acquisition of ALPR data was not an unreasonable search when it revealed the defendant's location on "106 occasions in thirty-three unique public locations over a four-and-a-half month period."[94] The court stated "there is no reasonable expectation of privacy in the information on license plates"; in fact, the "very purpose of a license plate number . . . is to provide identifying information to law enforcement and others."[95] The court also addressed and ultimately rejected the applicability of the mosaic theory, stating:

> Even in the aggregate, the ALPR cameras "capability to capture multiple shots of a single vehicle and/or store historical data does not approach the near-constant surveillance of cell-phone users" public and private moves that so concerned the Court in *Carpenter*. Rather, the technology is more akin to the conventional surveillance methods, such as security cameras, that the *Carpenter* Court was careful not to call into question.[96]

On the other hand, in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit did not answer the narrow question of whether

---

91. Carpenter v. United States, 585 U.S. 296, 312 (2018).

92. United States v. Brown, No. 19 CR 949, 2021 WL 4963602, at *3 (N.D. Ill. Oct. 26, 2021).

93. *Id.*

94. United States v. Bowers, 2:18-CR-00292-DWA, 2021 WL 4775977, at *4-*5 (W.D. Pa. Oct. 11, 2021) ("This limited data collection does not even begin to approach the same degree of information as that gathered in *Carpenter*.").

95. *Id.* at *3 (citing United States v. Ellison, 462 F.3d 557, 561-62 (6th Cir. 2006).

96. *Id.* (citing Carpenter, 585 U.S. 296, 316 (2018)); *see also* United States v. Toombs, 671 F.Supp.3d 1329, 1340-41 (N.D. Ala. 2023) (finding the officer only received one data point from his query; obtaining suspect's location at a discrete time while traveling on a public road was not an unreasonable search (distinguishing United States v. Knotts, 460 U.S. 276 (1983))).

ALPRs violate Fourth Amendment privacy interests; however, the technology at issue, drone surveillance, is a useful comparison.[97] In this case, the court found that aerial footage of the city, which was retained for at least forty-five days, was "a 'detailed encyclopedic,' record of where everyone came and went within the city during daylight hours over the prior month-and-a-half."[98] The retained drone surveillance allowed "[l]aw enforcement [to] 'travel back in time' to observe a target's movements, forwards and backwards."[99] Even though the data was only collected in twelve-hour increments, "the program enable[d] photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips."[100] Notably, the Court disregarded the fact that the drone surveillance did not follow individuals indoors because the resulting data still "enable[d] deductions about 'what a person does repeatedly [and] what he does not do,'" and thus revealed, "'an intimate window' into a person's associations and activities."[101]

Like drone surveillance, sufficient ALPR data would arguably allow deductions about a person's movements without following them indoors.[102] Although ALPRs are likely even more pervasive due to their twenty-four-hour-a-day surveillance, the state of ALPR technology in Indiana likely does not capture enough movement to enable such deductions; the cameras are sufficiently distant from one another and only capture data where they are located. If enough cameras were employed to produce a quantity of data points rivaling CSLI or drone footage, it would be more likely to invoke Fourth Amendment protection. But merely presenting the potential of the technology, especially when weighed against benefits to law enforcement, likely does not amount to an unconstitutional search.

B. Indiana's Article 1, Section 11

Although the language of the Fourth Amendment and Article 1, Section 11 ("Section 11") of the Indiana Constitution are identical, Indiana's analysis differs from the federal analysis.[103] First, Indiana imposes a standing requirement independent of privacy expectations;[104] to challenge a search as

97. *Beautiful Struggle*, 2 F.4th 330, 341 (4th Cir. 2021).

98. *Id.* at 341.

99. *Id.* (quoting *Carpente*r, 585 U.S. at 297).

100. *Id.* at 342 (quoting United States v. Jones, 565 U.S. 400, 415-17 (2012) (Sotomayor, J., concurring)).

101. *Id.* (quoting United States v. Maynard, 615 F.3d 544, 562-63 (D.C. Cir. 2010)).

102. CRUMP ET AL., *supra* note 10.

103. IND. CONST. art. I, § 11; Litchfield v. State, 824 N.E.2d 356, 359 (Ind. 2005) ("Indiana has explicitly rejected the expectation of privacy as a test of the reasonableness of a search or seizure.").

104. *Cf.* Rakas v. Illinois, 439 U.S. 128, 140 (1978) (explaining that federal standing inquiry is "properly placed within the purview of substantive Fourth Amendment law.").

unreasonable under Section 11, a defendant must show "ownership, control, possession, or interest in either the premises searched, or the property seized."[105]

Not only does the standing requirement distinguish Section 11 from the Fourth Amendment analysis, but the reasonableness analysis itself differs. Under Section 11, the court evaluates the "reasonableness of the police conduct under the totality of the circumstances"; Indiana's analysis is entirely objective and focuses on the police conduct, as opposed to the federal counterpart's focus on an individual's objective *and* subjective expectation of privacy.[106]

In addition, the totality-of-the-circumstances framework requires the court to attempt to "strike the proper balance between" the underlying competing interests:[107] limiting "excessive intrusions by the State into their privacy"[108] and "supporting the State's ability to provide 'safety, security, and protection from crime.'"[109] In light of these principles and any other relevant considerations, evaluating the reasonableness of a search requires a balancing of: "1) the degree of concern, suspicion, or knowledge that a violation has occurred, 2) the degree of intrusion the method of the search or seizure imposes on the citizen's ordinary activities, and 3) the extent of law enforcement needs."[110]

1. Section 11 Analysis.—There are two challenging aspects to bringing a Section 11 claim against ALPRs. First, to succeed on a facial challenge, the claimant has "the burden of demonstrating that there is no set of circumstances under which the statute can be constitutionally applied."[111] This heavy burden, along with the fact that a challenge would be against unclear government practices rather than a defined statute, causes a facial challenge to be somewhat impractical—it is difficult to apply a practice to any set of circumstances when the practice itself is unknown. By the same token, the public's inability to monitor law enforcement's use of ALPRs likely disallows an individual from bringing an as-applied challenge because they will be unable to prove whether law enforcement actually assembled the individual's location data in a way that

105. Peterson v. State, 674 N.E.2d 528, 534 (Ind. 1996) (finding that although defendant had an interest in the property seized, the defendant had no interest in the apartment searched because it was leased to his mother and sister, the mother paid rent, and mother had sole determination whether the defendant could reside at the apartment); Allen v. State, 893 N.E.2d 1092, 1096 (Ind. Ct. App. 2008) (finding that defendant was a trespasser and showed no legitimate right to the premises searched).

106. *Litchfield*, 824 N.E.2d at 359 (citing Moran v. State, 644 N.E.2d 536, 539 (Ind. 1994)).

107. Hardin v. State, 148 N.E.3d 932, 943 (Ind. 2020) ("It is because of concerns among citizens about safety, security, and protection that some intrusions upon privacy are tolerated, so long as they are reasonably aimed toward those concerns." (citing Holder v. State, 847 N.E.2d 930, 940 (Ind. 2006)).

108. *Id.* at 942-43 (citing State v. Washington, 898 N.E.2d 1200, 1206 (Ind. 2008); Marshall v. State, 117 N.E.3d 1254, 1261 (Ind. 2019)) ("And so we liberally construe . . . Section 11 to protect individuals.").

109. *Id.* at 943 (citing Holder v. State, 847 N.E.2d 930, 940 (Ind. 2006)).

110. Litchfield v. State, 824 N.E.2d 356, 361 (Ind. 2005).

111. Meredith v. Pence, 984 N.E.2d 1213, 1218 (Ind. 2013).

reveals private information.[112] In other words, establishing the presence of a search is a preliminary hurdle that is likely insurmountable, making it challenging to address any broader issues of misuse.

The second challenging aspect, which in some ways stems from the first challenge, regards the threshold issue of what constitutes a search. To properly understand the application of Section 11 to ALPRs, it is worth reiterating what aspect of ALPR technology should be defined as a "search." As previously mentioned, the search does not occur when the cameras photograph individual license plates or when the data sits idle in the database;[113] instead, the search arguably occurs when the long-term data is used to map out an individual's movements over a period of time, revealing private information about the individual.[114] Although it seems obvious that this information is not available to the public in the same way a license plate is exposed to public view, Indiana has not accepted or rejected, implicitly or explicitly, any form of the mosaic theory.[115] However, there is also support for the proposition that Section 11 provides greater protection than the Fourth Amendment.[116] For purposes of the analysis, it is assumed that Indiana recognizes that the assembly of long-term location information is a search, but it is important to recognize that this threshold issue could potentially be detrimental to the claim.

a. Standing.—The Indiana Supreme Court has recognized a privacy interest in a person's vehicle but noted that this interest does not "render [vehicles] beyond the reach of reasonable police activity."[117] However, because the proffered search involves the assembly of location information rather than the isolated capture of license plate numbers, the appropriate inquiry is whether an individual has an interest in their movements that could potentially reveal sensitive information. Again, there is no precedent to confirm Indiana recognizes this interest, but an individual's movements are within their control, and it is reasonable to believe that an individual has an interest in movements that can reveal sensitive information.

---

112. Smith, *supra* note 19 ("If there are no guidelines, how do we know it is not being abused?").

113. Wilkinson v. State, 743 N.E.2d 1267, 1270 (Ind. Ct. App. 2001) ("Suspicionless check of license plate numbers is not an improper search."); *See* Peterson v. State, 674 N.E.2d 528, 535 (Ind. 1996) (explaining that search connotes "prying into hidden places" but no explicit adoption of federal "plain view doctrine").

114. *See* Carpenter v. United States, 585 U.S. at 296, 311-12 (2018).

115. Zanders v. State, 118 N.E.3d 736, 741 n.4 (Ind. 2019), *remanded for further consideration in light of Carpenter*, 585 U.S. 296 (deciding the reasonableness of Fourth Amendment search of CSLI data on the grounds of harmless error; Court declined to reconsider the state constitutional claim, noting Section 11 does not depend on Fourth Amendment).

116. Linke v. Northwestern School Corp., 734 N.E.2d 252 (Ind. Ct. App. 2000), *vacated*, 763 N.E.2d 972 (Ind. 2002) (citing Moran v. State, 644 N.E.2d 536, 538 (Ind. 1994)); Peterson v. State, 674 N.E.2d 528, 533 (Ind. 1996).

117. Hardin v. State, 148 N.E.3d 932, 945 (Ind. 2020) (citing Taylor v. State, 842 N.E.2d 327, 334 (Ind. 2006)) ("Automobiles are among the 'effects' protected by … Section 11.").

b. Reasonableness.—

(i) Degree of suspicion.—Pursuant to a totality of the circumstances approach, the court "consider[s] all '. . . information available to [officers] at the time' of the search" when determining the degree of suspicion that a violation has occurred.[118] The Indiana Supreme Court has stated explicitly that "an important factor in evaluating a reasonable search is appropriate restriction on arbitrary selection of persons to be searched."[119] When license plate information is captured and assimilated into the larger database, it is done so indiscriminately; most of the detailed location information is stored for prolonged periods of time without attributable suspicion.[120] But the capture and mere storage of information is not the "search" being challenged, so the degree of suspicion depends on the information available to law enforcement when they subsequently assemble the information and cross-reference other databases.[121]

It is reasonable to infer that the Indiana Supreme Court would require officers to possess "articulable individualized suspicion" before accessing and assembling sensitive location information, as the Court has urged that this requirement appropriately balances citizens' privacy interests and law enforcement's needs.[122] But while law enforcement technically has the freedom to assemble location information indiscriminately, it would be difficult to use this mere possibility to succeed on a facial challenge. Although there is an opportunity for law enforcement to access and subsequently assimilate data about an individual who has not caused any suspicion, there is conversely a circumstance where the officer has reason to believe an individual has committed a crime, and the ALPR data could be useful in solving that crime. In the latter circumstance, the degree of suspicion is high and likely justifies accessing and assembling the information.

The complications arising from a facial challenge are evident in this prong. If an *innocent* individual were able to prove that law enforcement accessed their ALPR records and assembled the data in a way that revealed the privacies of their life, this prong would likely weigh in favor of the individual. However, because of the lack of oversight on law enforcement agencies' use of ALPR databases, individuals are unaware of whether and how their information is used.[123]

---

118. *Id.* at 943 (citing Duran v. State, 930 N.E.2d 10, 18 (Ind. 2010)).

119. Litchfield v. State, 824 N.E.2d 356, 364 (Ind. 2005).

120. *2019 ALPR Hit Ratio Report for Indianapolis Metropolitan Police Department by Vigilant Solutions*, MUCKROCK (Jan. 28, 2020), https://www.muckrock.com/foi/indianapolis-160/2020-vigilant-data-sharing-information-automated-license-plate-reader-alpr-indianapolis-metropolitan-police-department-86940/#file-840642 [https://perma.cc/NP4N-NR3F]; CRUMP ET AL., note 10, at 13.

121. *Litchfield*, 824 N.E.2d at 361 (applying "degree of suspicion" prong to ALPR search challenge).

122. *Id.* at 364 (requiring officers to possess articulable individualized suspicion before obtaining and searching through garbage); Baldwin v. Reagan, 715 N.E.2d 332, 337 (Ind. 1999) (requiring individualized suspicion of seat belt violation before stopping motorist).

123. Smith, *supra* note 19.

(ii) Degree of intrusion.—Focusing on the degree of intrusion caused by the *method* of the search emphasizes the importance of *how* officers conduct a search.[124] The intrusion is considered from the defendant's point of view, making a defendant's consent and ability to avoid the search relevant.[125] Moreover, examining the degree of intrusion into an individual's ordinary activities considers the intrusion into their physical movements and privacy.[126] For example, in traffic stop cases, Indiana courts have focused on the degree of intrusion into the defendant's physical movements,[127] whereas in trash-search and other cases, courts have focused on the intrusion into the defendant's privacy.[128] Both types of intrusions are relevant to the analysis, so although overall, there are differences between the Indiana and federal analyses, an inquiry into the degree of intrusion inevitably considers privacy expectations.[129] Because the interest at issue concerns a person's physical movements, analyzing the degree of intrusion essentially compares the extent to which law enforcement tracks a person in a vehicle against that person's privacy expectations and freedom of movement.

Individuals do not consent to the initial capture of their location information through ALPRs, nor are they asked for consent regarding any subsequent use of that information.[130] Moreover, to avoid ALPRs altogether, an individual would either have to map out the location of all readers and take alternate routes, drive a car that is not registered in their name, or avoid driving altogether. ALPR detection likely does not need to be entirely voluntary, but the lack of consent and inability to avoid ALPRs suggest a high degree of intrusion.[131]

However, practically, the degree of intrusion into an individual's privacy is likely low because it is improbable that law enforcement currently can use ALPR data to reveal an individual's everyday movements. In other words, the actual tracking is likely not persistent enough; ALPRs are scattered, and the relatively limited quantity prevents consistent revelation of an individual's movements over a prolonged period.[132] The fact that law enforcement only intrudes on someone's location information, which is observable by the public,

---

124. Hardin v. State, 148 N.E.3d 932, 945 (Ind. 2020).

125. *Id.* at 944 (citing Carpenter v. State, 18 N.E.3d 998, 1002 (Ind. 2014)); Duran v. State, 930 N.E.2d 10, 18 n.4. (Ind. 2010); State v. Gerschoffer, 763 N.E.2d 960, 969 (Ind. 2002).

126. *Hardin*, 148 N.E.3d at 944.

127. *Id.* at 944-45 (citing Austin v. State, 997 N.E.2d 1027, 1035-36 (Ind. 2013)); State v. Hobbs, 933 N.E.2d 1281, 1287 (Ind. 2010).

128. *Hardin*, 148 N.E.3d at 945 (citing *Duran*, 930 N.E.2d at 18; Litchfield v. State, 824 N.E.2d 356, 363-64 (Ind. 2005)).

129. *Hardin*, 148 N.E.3d at 944-45 (citing *Duran*, 930 N.E.2d at 18; *Litchfield*, 824 N.E.2d at 363-64).

130. Diaz & Levinson-Waldman, *supra* note 7.

131. *Cf.* Indiana v. Gerschoffer, 763 N.E.2d 960, 969 (Ind. 2002) (sobriety checkpoint need not be entirely voluntary, but the more avoidable it is, the less it interferes with liberty of drivers).

132. *See generally* Nelson, *supra* note 2.

also weighs in favor of a low degree of intrusion.[133] The revelation of intimate details, when the location information is assembled and compared with other data, is not observable by the public, but there still needs to be an ample number of cameras to actually paint a full picture.

In addition, the degree of intrusion into an individual's physical movements is low. Law enforcement's assembly of location data does not interfere with an individual's physical movements, as individuals are unaware of any assembly. In addition, law enforcement is not physically stopping anyone's vehicle with the technology.[134] While civil liberties organizations fear that the use of ALPRs can cause individuals to "become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance," this remains only a risk.[135]

(iii) Extent of law-enforcement needs.—"[L]aw-enforcement needs exist not only when officers conduct investigations of wrongdoing but also when they provide emergency assistance or act to prevent some imminent harm."[136] Law-enforcement needs refer to the "needs of the officers to act in a general way,"[137] but also to "act in a particular way and at the particular time they did."[138] The technology's effectiveness and potential deterring effects are relevant in determining the extent of law enforcement needs.[139]

Although law enforcement's general need to prevent and solve crime is recognized by society, that general need alone likely does not justify random searches into someone's location information because this "gives excessive discretion to engage in fishing expeditions," which the Indiana Supreme Court has expressly sought to prevent.[140] While recent data regarding the effectiveness of ALPRs is limited, a 2019 report for Indianapolis readers provides that of 1,164,281 plate detections, only 34,076 were hits.[141] In other words, less than 3% of detections triggered a hit, and whether those hits resulted in an arrest is unknown.

---

133. *Cf.* Carpenter v. State, 18 N.E.3d 998, 1002 (Ind. 2014) (quoting Moran v. State, 644 N.E.2d 536, 540 (Ind. 1994)) ("Houses and premises of citizens receive the highest protection.").

134. *See Gerschoffer*, 763 N.E.2d at 960.

135. CRUMP ET AL., *supra* note 10, at 8.

136. Hardin v. State, 148 N.E.3d 932, 946 (Ind. 2020) (citing *Carpenter*, 18 N.E.3d at 1002; Trimble v. State, 842 N.E.2d 798, 804 (Ind. 2006)).

137. *Id.* at 946-47 (citing Marshall v. State, 117 N.E.3d 1254, 1262 (Ind. 2019) (discussing the general need to enforce traffic-safety laws); Austin v. State, 997 N.E.2d 1027, 1036 (Ind. 2013) (discussing the general need to combat drug trafficking)).

138. *Id.* at 947 (citing Duran v. State, 930 N.E.2d 10, 19 (Ind. 2010)) (finding the specific needs were not pressing to execute arrest warrant because officers had shaky information on subject's location and no flight risk); Myers v. State, 839 N.E.2d 1146, 1154 (Ind. 2005) (search of vehicle upheld partly because elevated specific needs when driver was not under arrest and might have driven away)).

139. Indiana v. Gerschoffer, 763 N.E.2d 960, 970 (Ind. 2002).

140. Litchfield v. State, 824 N.E.2d 356, 364 (Ind. 2005).

141. *2019 ALPR Hit Ratio Report for Indianapolis Metropolitan Police Department by Vigilant Solutions*, *supra* note 120.

However, when the officer is notified of a hit and consequently assembles appropriate location data, the specific need to act quickly weighs in favor of constitutionality. Regarding deterrence, psychology studies confirm that people alter their behavior when they know they are being watched.[142] While this proposition can be used to argue that ALPRs chill the associational freedoms of innocent people, it similarly supports the argument that the cameras deter the commission of crimes.[143]

2. Related Indiana Precedent.—There have not yet been any challenges to law enforcement's use of ALPR data in Indiana. Although not directly on point, the defendant in *Maloney v. State* contended that "the viewing of [his] license plate was not improper, but the subsequent search of [his] personal records" was unconstitutional.[144] In *Maloney*, the law enforcement officer randomly checked the defendant's license plate number and discovered, through records shared by the Bureau of Motor Vehicles ("BMV"), that the vehicle's registered owner had a suspended license.[145] Because law enforcement was statutorily authorized to search records maintained by the BMV, the Indiana Court of Appeals held the search was reasonable.[146]

The challenge in *Maloney* is distinguishable from an ALPR challenge for several reasons. First, the statutory authorization the court relied on is inapplicable in the context of ALPRs because the BMV does not manage the ALPR database.[147] Second, the potential scope of ALPR data significantly exceeds the personal data maintained by the BMV;[148] although a mere license plate number is comparable, the sensitive information that can be deduced from the ALPR's recording of plate number, time, and precise location is unconventional. Third, and for similar reasons, it is expected that the BMV possesses the records discussed in *Maloney*, specified in the relevant statute, and shares such records with law enforcement.[149]

Although not directly addressing ALPR technology, in *McCowen v. State*, the defendant challenged law enforcement's procurement of his cell phone records.[150] In this situation, the Indiana Court of Appeals found the police had a great degree of suspicion that the defendant had information about a missing individual and that the defendant's movements would be informative of the

142. CRUMP ET AL., *supra* note 10, at 8.

143. *Id.*

144. Maloney v. State, 872 N.E.2d 647, 650 (Ind. Ct. App. 2007) (internal quotation marks omitted).

145. *Id.* at 648.

146. *Id.* at 652; IND. CODE § 9-14-3-5 (repealed 2016); IND. CODE § 9-14-3.5-10 (repealed 2016).

147. IND. INTEL. FUSION CTR, *supra* note 22.

148. IND. CODE § 9-14-13-2 (2016) (effectively replacing the statute discussed in Maloney v. State, 872 N.E.2d 647 (Ind. Ct. App. 2007)) (listing social security number, federal identification number, driver's license number, etc.).

149. *Id.*

150. McCowan v. State, 10 N.E.3d 522, 525 (Ind. Ct. App. 2014), *rev'd on other grounds*, 27 N.E.23d 760 (Ind. 2015).

missing person's whereabouts.[151] The degree of intrusion was minimal because law enforcement requested records from the cell phone provider as a routine part of their recordkeeping, the defendant did not have to surrender his phone, and the request did not disrupt his activities.[152] Additionally, the police only requested records of his activity between the eighteen hours.[153] Finally, the court found the extent of law enforcement needs was great because the police searched for a recently missing individual when they requested the records.[154]

McCowen reaffirms the idea that the mere capture and passive accumulation of ALPR data is likely not a "search" but instead considered routine recordkeeping.[155] However, manipulating the data to reveal a comprehensive record of an innocent individual's past should not be considered routine recordkeeping. The fundamental obstacle preventing innocent individuals from bringing a successful challenge that will effectually protect their privacy is, given the lack of transparency, the unlikeliness that an innocent individual will ever be informed of law enforcement's actions.[156] Consequently, innocent individuals must tolerate the invasion of privacy until the technology is so pervasive that the proper defendant can challenge law enforcement's warrantless search and subsequent assembly of ALPR data, revealing the intimate details of the defendant's whereabouts.[157]

C. No Constitutional Protection: Problem of Degree

Both Fourth Amendment federal claims and Section 1, Article 11 State claims essentially fail because of the minimal degree of intrusion.[158] While the mosaic theory applies to the *capabilities* of ALPR technology, it is not currently applicable to its actual implementation. Federal claims have failed because of the minimal data points from ALPR searches, which were submitted as evidence. Knowing a few places where someone publicly travels cannot be reasonably considered a violation of privacy, especially considering the established principle that there is no reasonable expectation of privacy for someone traveling in an automobile on public thoroughfares.[159] State claims will likely fail for the same reason, as Article 1, Section 11's test of reasonableness explicitly addresses the degree of intrusion.[160]

---

151. *Id.* at 534.
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*
156. *See* Smith, *supra* note 19.
157. *See* Ramirez v. State, 174 N.E.3d 181 (Ind. 2021); Zanders v. State, 118 N.E.3d 736 (Ind. 2016). Circumstances will also have to overcome the exigent circumstances exception to the warrant requirement. *Id.*
158. *See generally* Carpenter v. United States, 585 U.S. 296, 311-13 (2018); Litchfield v. State, 824 N.E.2d 356, 361 (Ind. 2005).
159. United States v. Knotts, 460 U.S. 276, 281 (1983).
160. Litchfield v. State, 824 N.E.2d 356, 361 (Ind. 2005).

In other words, until a case demonstrates that ALPR data is far more comprehensive than previously shown, law enforcement will continue collecting location information on individuals. The timeline for reaching a level of surveillance that warrants constitutional scrutiny will vary depending on the extent to which local or state authorities have advanced in deploying ALPR technology.

As previously mentioned, implementation of this technology shows no signs of stopping, and it is reasonable to expect ALPR usage will grow exponentially; while there may only be a couple hundred cameras in Indianapolis today, there could be a couple thousand in the near future.[161] The more cameras there are, the more data points the government can collect about each individual, and "[a]s technological capabilities advance, . . . confidence that the Fourth Amendment (as currently understood by the courts) will adequately protect individual privacy from government intrusion diminishes."[162]

Put differently, the degree of tolerance for government intrusion into privacy, shaped by the current circumstances, essentially sets the standard for society's initial baseline of what qualifies as a reasonable expectation of privacy.[163] As the government's use of ALPRs incrementally, and likely inconspicuously, expands, one could argue that society's reasonable expectation of privacy expands simultaneously, so long as no one challenges the technology. Eventually, when ALPR usage becomes so pervasive that it consistently captures an individual's location data numerous times throughout the day, the government will have wide latitude to argue that such surveillance fits within the boundaries of society's reasonable expectation of privacy.[164]

The question follows: How far are Americans willing to allow government surveillance technologies to encroach upon their daily lives before deciding that this violates a reasonable expectation of privacy? To prevent the passage of time from defining this standard, policymakers and citizens must voice their concerns regarding the trade-offs between security and privacy.[165] Truly securing the bounds of a reasonable expectation of privacy must come in the form of legislation.

---

161. Lavernacole, *Automatic License Plate Recognition (ALPR) Market Size, Growth, Forecast 2023–2030*, MEDIUM (Nov. 10, 2023), https://medium.com/@lavernacole2023/automatic-license-plate-recognition-alpr-market-size-growth-forecast-2023-2030-f6f03b3018ff [https://perma.cc/NM6Q-CN4L].

162. United States v. Tuggle, 4 F.4th 505, 527-28 (7th Cir. 2021) (citing Kyllo v. United States, 533 U.S. 27, 33-34 (2001)).

163. *See id.*

164. *See id.* at 527 (citing United States v. Jones, 565 U.S. 400, 404-11 (2012)).

165. *See* Diaz & Levinson-Waldman, *supra* note 7.

III. PROPOSED LEGISLATION

Because of the lack of constitutional protection, the best solution for ensuring law enforcement does not invade our privacy via ALPR data while preserving its crime-fighting benefits is by enacting statutory restrictions. Indiana currently lacks any legislation or statewide guidelines regarding ALPRs.[166] At least sixteen other states have enacted legislation; the statutory language, for the most part, varies greatly.[167] Indiana's legislation should be tailored to the specific goals of ALPR usage in Indiana. The proposed legislation will primarily address ALPR use by law enforcement agencies.[168]

A. Restrictions Based on Intended Use

The restrictions on ALPR data access should depend on law enforcement's intended use. While an officer should be able to easily check a plate number during a routine traffic stop to promote the officer's safety, it should be more difficult to retain records of an individual car for purposes of long-term tracking.[169] In addition, the sensitivity of the data necessitates a higher bar for the distribution of the data. Regardless of the intended use, the ALPR operator should be required to submit the reason for inquiry into the system.

1. Quick Access: Legitimate Law Enforcement Purposes.—Law enforcement's access to the information collected by ALPRs should be statutorily restricted to "legitimate law enforcement purposes." This will allow ALPRs' crime prevention and solving capabilities to persist while mitigating the invasion of innocent individuals' private data. The existing Indiana State Police ALPR policy ("ISP Policy") currently restricts the utilization of hot lists to legitimate law enforcement purposes; however, this term is not defined.[170]

A statutory definition of "legitimate law enforcement purposes" should delineate the primary objectives of ALPRs while maintaining a nonexclusive character. Providing context-based examples in the definition will illuminate the intended applications of ALPR data usage.[171] However, acknowledging that the

---

166. Smith, *supra* note 19.

167. *Automated License Plate Readers: State Statutes*, NAT'L CONF. STATE LEGISLATURES (Feb. 3, 2022), https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes [https://perma.cc/QV6K-8VMJ].

168. *See, e.g.*, ARK. CODE 12-12-1803(b) (2017) (defining separate uses for parking enforcement entities and Department of Transportation); ME. REV. STAT. tit. 29, § 2117-A(3) (2013) (creating exceptions for the Department of Transportation and Department of Public Safety).

169. *Comprehensive Legislation on Automatic License Plate Readers: Overview*, *supra* note 9.

170. *Standard Operating Procedure: License Plate Reader*, IND. STATE POLICE (Aug. 18, 2023), https://public.powerdms.com/Ind3899/documents/2007753/ENF017%20License%20Plate%20Reader [https://perma.cc/W9U4-JD4V].

171. *Comprehensive Legislation on Automatic License Plate Readers: Overview*, *supra* note 9.

list is not exhaustive will afford law enforcement flexibility if the technology proves advantageous in unforeseen ways not initially contemplated. The absence of evidence indicates that Indiana law enforcement utilizes ALPRs for non-investigative purposes, so the list should only pertain to investigative use.[172]

2. Retaining Data/Long-Term Tracking: Thirty Days.—The information retention limit within other states' applicable statutory schemes ranges from three minutes[173] to thirty months;[174] there is nearly always an exception provision allowing for an extended retention period for specific circumstances or upon request. The existing ISP Policy allows for thirty days of data retention "before being purged from the system," unless collected information is placed into the incident management system.[175] Two of the three proposed Indiana bills suggested a twenty-four-hour retention period unless the situation satisfies specific requirements.[176] The third bill suggested a thirty-day retention period with largely the same exceptions.[177]

A thirty-day retention period balances crime-stopping benefits while mitigating any negative privacy impacts.[178] Rather than immediately purging data, thirty days of retention allows law enforcement to maintain both the real-time and archival benefits of ALPRs.[179] Law enforcement would be able to use limited historical data, but the data would not date so far back that an assembly could reveal an extensive pattern of an individual's whereabouts. Instead, law enforcement can use short-term patterns to identify areas of crime and implement preventative measures when appropriate.[180] To retain the data for longer than thirty days and subsequently access this historical data, law enforcement should be required to obtain a warrant or submit a preservation request. This requirement will ensure law enforcement is validly exercising their invasion on an individual's privacy by "[placing] obstacles in the way of a too permeating police surveillance."[181]

---

172. ARK. CODE § 12-12-1803(b) (2017) (controlling access to secured areas, verification of registration, logs, and other compliance data for highway travel).

173. N.H. REV. STAT. § 261.75-b(VIII) (2017).

174. GA. CODE § 35-1-22(b) (2018).

175. *Standard Operating Procedure: License Plate Reader*, supra note 170.

176. S.B. 238, 119th Gen. Assemb., 1st Reg. Sess. (Ind. 2015); S.B. 417, 118th Gen. Assemb., 2nd Reg. Sess. (Ind. 2014) (exceptions include if obtained under warrant, is relevant to ongoing criminal investigation, location or identity of fugitive, location of missing person, commission of crime, or person who owns license plate requests retention).

177. H.B. 1558, 120th Gen. Assemb., 1st Reg. Sess. (Ind. 2017).

178. *See* Diaz & Levinson-Waldman, *supra* note 7.

179. Joel F. Shultz, *How ALPR Data Drives Intelligence-Led Policing*, LEXIPOL (May 3, 2018), https://www.police1.com/police-products/traffic-enforcement/license-plate-readers/articles/how-alpr-data-drives-intelligence-led-policing-BQmAMSJFCHtld7lc/ [https://perma.cc/5S99-42GH].

180. *Id.*

181. Carpenter v. United States, 585 U.S. 296, 305 (2018) (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

3. Disclosing Data: Confidentiality.—Disclosure of ALPR data should be limited due to the sensitive nature of the information.[182] Disclosing information is distinct from retaining information, as the data can be retained in the database without being distributed or accessed. Without restrictions, the mass collection of data can be fed into even larger regional databases or shared with private companies; once a law enforcement agency shares the data, it can lose control of how it is used, stored, and further distributed.[183]

Restricting law enforcement's sharing abilities to legitimate law enforcement purposes and in response to specific requests from other agencies allows agencies to support each other in solving crime while ensuring innocent individuals' data is not carelessly disseminated.[184] To further protect individual privacy, there should be a higher bar to disclose information to non-law enforcement agencies. The data should only be able to be disclosed to specified recipients pursuant to a valid court order. Establishing a heightened threshold for disclosing information to law enforcement agencies and the general public will reinforce individual privacy protections.[185]

B. Ensuring Transparency

Requiring agencies to create and adopt policies will provide guidance and help ensure internal agency conduct does not violate individual privacy. [186] These policies, along with statistical data resulting therefrom, should be published so citizens can see how law enforcement uses their location information and, when necessary, challenge any practices they believe to be violative of their privacy.[187]

Only authorized law enforcement personnel trained, certified, and subjected to a background check should have access to the ALPR database.[188] The adopted policy should describe the training and certification process. In addition, the policy should describe how the agency will maintain statistical data regarding ALPR usage and retention to hold agencies accountable for their use.[189] All queries in the database should be subject to auditing, so the statistical data

---

182. *Cf.* IND. CODE § 9-14-13-2 (2024) (restrictions on the BMV's disclosure of sensitive personal information); *but see* IND. INTEL. FUSION CTR, *supra* note 22 (BMV does not manage ALPR database).

183. CRUMP ET AL., *supra* note 10, at 18.

184. *Id.*

185. *See* Albert Gidari, *Public Access to Smart Data*, CTR. FOR INTERNET AND SOC'Y (Sept. 25, 2017, 10:14 AM), https://cyberlaw.stanford.edu/blog/2017/09/public-access-smart-data [https://perma.cc/EU6Q-Q39Y].

186. *E.g.*, MD. CODE PUBLIC SAFETY § 3-509(c) (2023); MONT. CODE ANN. § 46-5-117(2)(d)(i) (2017); NEB. REV. STAT. § 60-3206(1)-(2) (2018); N.C. GEN. STAT. § 20-183.30 (2015).

187. Diaz & Levinson-Waldman, *supra* note 7.

188. *ALPR FAQs*, *supra* note 30.

189. *Comprehensive Legislation on Automatic License Plate Readers: Overview*, *supra* note 9.

should be logged and stored in a format that permits auditing.[190] This log should include details about automated ALPR alerts, including the reason for the alert, whether any information was shared with other agencies, and the outcome of the alert.[191] The logs should track every time an officer seeks to access historical ALPR data, specifying the officer and crime being investigated.[192] Maintaining statistical data of this nature will also allow for thorough empirical studies on the efficacy of ALPRs.[193]

C. Example Statutory Language

In order to safeguard individuals' privacy against the potential misuse of ALPRs, it is imperative to incorporate the following provisions into Indiana law:

A. Definitions
   1. "Active data" refers to data uploaded to individual automated license plate reader systems before operation or data gathered during the operation of an automatic license plate reader. "Active data" does not include historical data.
   2. "Legitimate law enforcement purposes" includes[194] identifying a vehicle that is stolen, associated with a wanted, missing, or endangered person, registered to a person against whom there is an outstanding warrant, in violation of commercial trucking requirements, involved in case-specific criminal investigative surveillance, involved in a homicide, shooting, or other major crime or incident, or in the vicinity of a recent crime and may be connected to that crime.[195]
   3. "Captured plate data" means the global positioning system coordinates, dates and times, photographs, license plate numbers, and any other data collected by or derived from an automated license plate reader, including active and historical data.
   4. "Historical data" refers to license plate data that is stored in an automated license plate reader database, including data retained beyond 30 days.

B. Accessing Data
   1. Captured Data

---

190. *See* MD. CODE ANN., PUBLIC SAFETY § 3-509(c) (2023).

191. Diaz & Levinson-Waldman, *supra* note 7.

192. *Id.*

193. *Comprehensive Legislation on Automatic License Plate Readers: Overview*, *supra* note 9.

194. *A Guide to Reading, Interpreting, and Applying Statutes*, WRITING CTR. GEO. U. LAW CTR. 5 (2017), https://www.law.georgetown.edu/wp-content/uploads/2018/12/A-Guide-to-Reading-Interpreting-and-Applying-Statutes-1.pdf [https://perma.cc/SY9S-XTUU] (presumption of nonexclusive "include").

195. *See* MONT. CODE ANN. § 46-5-117(2)(d)(iii) (2017); N.H. REV. STAT. § 261.75-b (2017).

a. Operation of a license plate reader and access to captured plate data by a law enforcement agency must be for legitimate law enforcement purposes only.
b. The operator must submit the reason for inquiry into the system in accordance with the agency's policy.

2. Historical Data
a. Law enforcement may not access historical data without a warrant.

C. Data Retention
1. Captured license plate data may not be preserved for more than 30 days after the date that it is captured, unless
a. The captured data was obtained under a warrant; or
b. Pursuant to a valid preservation request.
2. A preservation request may be submitted by
a. Law enforcement agency, or
b. The person whom a license plate was issued.
c. A party to a pending or potential litigation.
3. A preservation request must specify in a sworn written statement:
a. The location of the particular camera or cameras for which captured license plate data must be preserved;
b. The particular license plate for which captured license plate data must be preserved; and
c. The date and time frames for which captured plate data must be preserved.
4. One year from the date of the initial preservation request, the captured license plate data obtained by an automatic license plate reader system must be destroyed, unless another preservation request is submitted within the 1-year period, in which case the 1-year retention period will be reset.

D. Data disclosure
1. Law enforcement agencies may exchange or share captured license plate data with other law enforcement agencies for law enforcement purposes upon request.
2. A governmental entity or defendant in a criminal case may apply for a court order for disclosure of captured plate data, which shall be issued by the court if the governmental entity or defendant in a criminal case offers specific and articulable facts showing that there are reasonable grounds to believe the captured license plate data is relevant and material to the criminal or civil action.
3. Captured plate data is otherwise confidential and may not be sold or transferred by a law enforcement agency to another person.

E. Policy
   1. Any law enforcement agency deploying an automated license plate reader shall adopt and publish a written policy for the use and operation of such system.
   2. The policy shall include:
      a. Procedures for training law enforcement officers in the use of captured license plate data consistent with this Code section;
      b. An audit process to ensure that information obtained through an automated license plate reader is used only for legitimate law enforcement purposes; and
      c. Any other subjects related to automated license plate reader use by the law enforcement agency.

CONCLUSION

As the prevalence of automated license plate readers continues to expand, it becomes increasingly important to address the potential erosion of privacy rights. Instead of waiting for privacy infringements to become serious enough to invoke obvious constitutional protection, Indiana policymakers should proactively safeguard the interests of its citizens. To achieve this, Indiana should consider enacting legislation that:

(1) Restricts law enforcement's access to ALPR data, specifying the permissible purposes and retention periods;

(2) Mandates all local law enforcement agencies to establish transparent protocols for the operation and utilization of ALPR technology;

(3) Demands the publication of statistical data to shed light on the actual usage of ALPR technology; and,

(4) Calls for an audit of relevant records to ensure compliance and accountability.

By establishing clear guidelines, checks, and balances for the use of surveillance technologies like ALPRs, we can protect our individual freedoms and maintain the delicate equilibrium between security and privacy. Under the proposed legislation, Indiana's law enforcement agencies, and by extension, the citizens of Indiana, can enjoy the crime-prevention advantages of ALPR technology, all the while maintaining a robust safeguard against unwarranted government intrusion into individuals' privacy. Through a combination of vigilant public awareness, responsible policymaking, and the active protection of our rights, we can navigate the ever-evolving landscape of privacy in the digital age.