Richmond Journal of Law & Technology

Volume 25 | Issue 3 Article 1

3-1-2019

Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia

Julia M. Brooks
University of Virginia School of Law

Richmond Journal of Law & Technology Volume XXV, Issue 3

DRAWING THE LINES: REGULATION OF AUTOMATIC LICENSE PLATE READERS IN VIRGINIA

Julia M. Brooks*

Cite as: Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia*, 25 RICH. J.L. & TECH., no. 3, 2019.

* *Juris Doctor*, University of Virginia School of Law. The author sincerely thanks Nicole Allaband, Lindsey Rhoten, and the entire editorial board at the *Richmond Journal of Law and Technology* for their diligent work on this publication.

ABSTRACT

Since the 1990s, police departments and private companies across America have located vehicles and tracked individuals using automatic license plate readers. Part I provides an introduction to these readers and their use by law enforcement agencies. The problems with the use of these readers and the substantial relationship between public and private actors in their use are discussed in Part II. Part III discusses the options on how to regulate both these readers and the data collected through their use. Part III also examines the potential impact of Neal v. Fairfax County Police Department*, a recent Supreme Court of Virginia case which has the potential to effectively ban automatic license plate readers in the Commonwealth and proposes a solution for this industry's advancement.*

I. THE AUTOMATIC LICENSE PLATE READER INDUSTRY

[1] Every day, automatic license plate readers (ALPRs) capture images of thousands of vehicles without the owners' consent or knowledge. Although you may not have realized it at the time, you have seen an ALPR. 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.

[2] ALPRs are seemingly innocuous pieces of technology. They are cameras that scan license plates on all passing cars regardless of whether the driver has committed any infractions.[1] Within a single minute, one reader can scan thousands of plates.[2] The reader takes a picture of each vehicle's license plate.[3] This picture may include the entire vehicle and driver. The photograph is saved, along with the time and location of the scan, onto a searchable database.[4] Regardless of whether the operator of the scanned vehicle has committed an infraction, law enforcement can

[1] *See You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements*, 4 ACLU (2013), [hereinafter *You Are Being Tracked*] https://www.aclu.org/other/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements [https://perma.cc/QY43-GX62] (explaining that license plate readers use cameras to capture a photograph of "each and every" license plate).

[2] *See* Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/ [https://perma.cc/JC7W-W2LD].

[3] *See id.*(stating that license-plate readers are "reading the license plates of every vehicle, parked or moving, that the cruiser passes").

[4] *See id.*(stating that license-plate scans are "stored in databases and can be searched by license plate number, turning up photos [of] every sighting of a particular vehicle—including the time and location of each sighting").

easily determine the vehicle's owner using a single scan and a separate database connecting identities to license plate numbers.[5] The scans are hypothetically deleted from the database at a later date.[6]

[3] Police-operated ALPRs simultaneously conduct automatic background checks on vehicles' owners.[7] This background check is intensive and searches files from the National Crime Information Center on the vehicle and license plate, as well as wanted persons, protection orders, missing persons, gangs, known and appropriately suspected terrorists, persons on supervised release, immigration violators, and sex offenders.[8] In one case, a man was pulled over following an ALPR scan that revealed an active warrant for the owner of the vehicle's brother.[9] The results of the background check are sent immediately to the ALPR's operating officer.[10] For example, if there is a *hit*, an alert that there is an outstanding warrant for the vehicle's owner, then the officer executes a traffic stop.[11]

---

[5] Use of databases connecting license plate numbers to names is regulated under the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–25. The exceptions to this law are exhaustive, however, and essentially allow access by anyone capable of operating an ALPR. *See* 18 U.S.C. §§ 2721–25 (2018).

[6] *See* Waddell, *supra* note 2, at 16 (explaining that some states' law enforcement agencies delete license-plate reader data from their systems).

[7] *See License Plate Reader Technology Enhances the Identification, Recovery of Stolen Vehicles*, 13 CJIS LINK 3–4, (Sept. 2011), [*hereinafter License Plate Reader Technology*] https://www.hsdl.org/?view&did=728581 [https://perma.cc/GN43-SHAD] (discussing the use of National Crime Information Center (NCIC) data with ALPR scans).

[8] *See id.* at 3.

[9] *See* United States v. Lurry, No. 2:09-cr-20312-JPM, 2010 U.S. Dist. LEXIS 118494, at *2–3 (W.D. Tenn., Nov. 8, 2010).

[10] *See License Plate Reader Technology*, *supra* note 7, at 3–4.

[11] *See id*. at 3–4 (noting that automated background checks can be executed very quickly and can be done by traffic patrol vehicles, which enables officers on duty to react quickly in response).

[4] ALPR use is growing quickly across the country.[12] According to a Department of Justice survey, more than three-quarters of police departments serving populations of over 100,000 residents utilized ALPRs in 2013.[13] In contrast, only forty-eight percent of these same departments reported ALPR use in 2007.[14] This growth has been spurred by the device's plummeting prices and more than $50 million in grants to local police departments from the Department of Homeland Security.[15]

[5] These readers have been incredibly effective tools against crime. For example, in 2016, St. Louis Police used stored scans to locate and track a stolen vehicle.[16] Officers located the vehicle and were nearly killed by the suspect.[17] When later interviewed, St. Louis Police Chief Sam

[12] *See* Brian A. Reeves, *Local Police Departments*, *2013: Equipment and Technology*, BJS BULLETIN 4, (July 2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf [https://perma.cc/E23E-9L62].

[13] *See id.* at 4.

[14] *See* DAVID J. ROBERTS & MEGHANN CASANOVA, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE: TECHNICAL CENTER, AUTOMATED LICENSE PLATE RECOGNITION (ALPR) USE BY LAW ENFORCEMENT: POLICY AND OPERATIONAL GUIDE 3 (2012), https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf [https://perma.cc/6NYU-T6FL].

[15] *See* Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, WALL ST. J., Sept. 29. 2012, http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html [https://perma.cc/SS7B-Z45S]; *see also Reduced Prices for License Plates* [sic] *Readers Attracts More Buyers*, HOMELAND SECURITY NEWS WIRE (Jan. 24, 2012), [hereinafter *Reduced Prices for License Plates*] http://www.homelandsecuritynewswire.com/srlet20120124-reduced-prices-for-license-plates-readers-attracts-more-buyers [https://perma.cc/M3PP-24V6] (stating that the price of an ALPR system has fallen from an initial cost of $24,000 to $17,000 as of January 2012).

[16] *See* Kelly Davis, *How License Plate Recognition Cameras Help Police Solve Crimes*, KMOV.COM (Dec. 14, 2016), https://www.kmov.com/news/how-license-plate-recognition-cameras-help-police-solve-crimes/article_51fc37e2-c684-5b0c-a063-69cb2c8a4a83.html [https://perma.cc/NW35-KHG4].

[17] *See id.*

Dotson praised the department's ALPRs.[18] He said that without the readers, the police "wouldn't have been drawn to this vehicle so [they] had a chance to take a criminal off the streets. [They have] taken hundreds of criminals off the streets because of the technology, it works."[19]

[6] This was far from an isolated incident. In Coral Springs, Florida, police used stored ALPR scans to build a murder case after they discovered the body of a young woman dumped in the woods.[20] Across the country, countless stolen cars have been recovered, illegal guns confiscated, and suspects fleeing warrants located.[21] The police department of Hollywood, Florida, increased its reader program four-fold in 2016 due to its success.[22] A spokesman for the city police department stated that, as a result of the readers, they have "caught murder suspects [and] burglars."[23]

[7] A neighboring police department had similar results, saying that the program has "worked spectacularly" and that they have been used to solve dozens of major crimes with very little information.[24] They pointed to one illustrative case where a bank robber was identified by eyewitnesses only as "a white man with a white T-shirt and possibly blonde hair."[25] Police located the suspect's vehicle and arrested him

[18] *See id.*

[19] *Id*.

[20] *See* Lisa J. Huriash, *License Plate Readers are Solving Crimes, Cities Say*, SUN SENTINEL (Jan. 22, 2016, 5:12 PM), https://www.sun-sentinel.com/local/broward/fl-coral-springs-license-plates-20160122-story.html [http://perma.cc/8KZG-P7EC].

[21] *See id.*

[22] *See id.*

[23] *Id.*

[24] *See id.*

[25] Huriash, *supra* note 20.

within three days using stored ALPR scans.[26] Countless examples of successful ALPR use exist and continue to occur on a daily basis.[27]

II. PROBLEMS WITH ALPR USE

[8] Despite the obvious benefits, ALPRs may be used in ways that limit civil liberties and constitutional freedoms even when they are operated properly. The D.C. Circuit's discussion of GPS trackers in *United States v. Maynard* highlights the hazards inherent in ALPR use:

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[28]

[9] When a law enforcement agency can find out exactly where you are on a given day at a given time and can compile enough information to determine your routines, your privacy is compromised, and your First Amendment rights are chilled.[29] This compromise is the primary concern for advocates of greater regulation of ALPR systems.[30] The systems' "active use" to take pictures of individuals' license plates and conduct background checks without probable cause or reasonable suspicion is not

[26] *See id.*.

[27] *See, e.g.*, *Platesearch*, VIGILANT SOLUTIONS, INC., [hereinafter *Platesearch*] https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/ [https://perma.cc/94Y8-AX46] (offering one type of successful ALPR service).

[28] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[29] *See id.* at 560.

[30] *See, e.g.*, *You Are Being Tracked*, *supra* note 1, at 24 (arguing that the use of license plate data raises several concerns).

necessarily problematic.[31] The systems' "passive use," where scans are stored along with the location, date, and time at which the image was captured, has much greater potential for harm.[32] Active use of ALPRs is widely accepted and has been approved by courts or legislatures numerous times over the years.[33] This is because license plates are in public view, and information obtained through a single ALPR scan, such as any outstanding warrants of the owner are public as well.[34] As a result, officers need absolutely no suspicion of a crime before doing an initial active scan.[35] However, scans are not foolproof, and some states have specifically noted that a positive scan is not necessarily sufficient to

[31] *See* United States v. Miranda-Sotolongo, 827 F.3d 663, 667 (7th Cir. 2016) (finding that performing a background check without cause based off of a license plate number does not implicate the Fourth Amendment).

[32] *Cf.* United States v. Maynard, 615 F.3d 544, 558–63 (D.C. Cir. 2010) (holding that the compilation of prolonged GPS surveillance data reveals far more information and a more complete picture of an individual's movements and patterns than short-term surveillance).

[33] *See, e.g., Miranda-Sotolongo*, 827 F.3d at 667–68 (holding that a police officer's check of a vehicle registration in a database is not a Fourth Amendment search); United States v. Diaz-Castaneda, 494 F.3d 1146, 1152 (9th Cir. 2007) (same); United States v. Ellison, 462 F.3d 557, 561–63 (6th Cir. 2006) (same); People v. Bushey, 75 N.E.3d 1165, 1166, 1169 (N.Y. 2017) (same and adding that the practice also does not implicate New York state law).

[34] *See, e.g.*, *Miranda-Sotolongo*, 827 F.3d at 667–68 (upholding a police officer's check of a license plate without reasonable articulable suspicion because no Fourth Amendment search occurred).

[35] *See Ellison*, 462 F.3d at 561–63 (upholding arrest following license plate scan and background check without prior suspicion).

initiate a traffic stop.[36] Otherwise, active ALPR use by law enforcement is essentially unregulated.[37]

[10] In contrast, passive ALPR use has been regulated by a handful of states and numerous law enforcement agencies.[38] A handful of jurisdictions limit the amount of time a scan can be stored before it must be deleted.[39] Some states impose additional burdens, such as reasonable suspicion or a brief affidavit, on officers attempting to access scan databases.[40] Passive ALPR use will likely be completely prohibited in Virginia pending the outcome of a remanded Virginia Supreme Court case.[41] In the meantime, many Virginia police departments have internal policies voluntarily limiting their passive use.[42]

---

[36] *See, e.g.*, MONT. CODE ANN. § 46-5-117(2)(d)(vi) (2017) ("a positive match by a license plate reader alone does not constitute reasonable suspicion as grounds for a law enforcement officer to stop a vehicle").

[37] *See Automated License Plate Readers: State Statutes,* NAT'L CONF. STATE LEGISLATURES (Nov. 6, 2018), [hereinafter *Automated License Plate Readers: State Statutes*] http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/JKH6-5LMF].

[38] *See id.*

[39] *See id.*

[40] *See* State v. Donis, 723 A.2d 35, 56 (N.J. 1998); *see also Automated License Plate Readers: State Statutes*, *supra* note 37.

[41] *See* Covington & Burlington, *Virginia Supreme Court Holds that License Plate Readers Collect Personal Information*, INSIDE PRIVACY (May 7, 2018), https://www.insideprivacy.com/united-states/litigation/virginia-supreme-court-holds-that-police-license-plate-readers-collect-personal-information/ [https://perma.cc/357Q-YP3W] (stating that this Virginia Supreme Court case held that a license plate number is not personal information, but that the license plate image and other associated data are personal information under the Act).

[42] *See* Allison Klein, *Virginia Limits Use of License-Plate Cameras*, WASH. POST (Mar. 7, 2013), https://www.washingtonpost.com/local/virginia-limits-use-of-police-license-

[11] However, use of ALPRs is not limited to government agents.[43] Vaas International Holdings, Inc., is a private corporation that owns networks devoted to the aggregation of ALPR scans.[44] One such network, Vigilant Solutions, is solely for law enforcement use.[45] The other network, however, Digital Recognition Network ("DRN") is solely for use by private entities and reportedly contains billions of scans and adds approximately 160,000 million each month.[46] DRN claims it has captured "a large majority" of plate data from vehicles registered in the United States.[47]

[12] DRN's primary purpose is to assist with the recovery of stolen or repossessed vehicles.[48] It does not limit itself to this purpose, however, and shares its data with other Vaas International-owned networks including the National Vehicle Location Service (NVLS) and Law Enforcement Archival Reporting Network.[49] NVLS is accessible to more than 3,500 state and federal law enforcement agencies, 25,000 law enforcement investigators, and adds at least 1,000 new members each

plate-cameras/2013/03/07/f1344c00-876d-11e2-98a3-b3db6b9ac586_story.html?utm_term=.cdfa599e784e [https://perma.cc/VQ77-EQN3].

[43] *See Platesearch*, *supra* note 27.

[44] *See Overview*, VAAS INT'L HOLDINGS, INC., http://vaasinternational.net/ [https://perma.cc/U9NT-MFT4].

[45] *See Platesearch*, *supra* note 27.

[46] *See You are Being Tracked*, *supra* note 1; *see also Live Alerts: Find Vehicles of Interest*, DIGITAL RECOGNITION NETWORK, https://drndata.com/live-alerts [https://perma.cc/HR95-6EJN].

[47] *You are Being Tracked*, *supra* note 1.

[48] *See Automotive Recovery*, DIGITAL RECOGNITION NETWORK, https://drndata.com/automotive-recovery [https://perma.cc/9LYA-EVUQ].

[49] *See* Brian Shockley, *A Case Study on License Plate Recognition (LPR): Coral Springs Police Department,* CRIME MAPPING & ANALYSIS NEWS: A POLICE FOUND. PUBLICATION (Fall 2015).

month.[50] Billions of scans collected by private individuals, without any concern about the constitutionality of their actions, are accessible to the thousands of participating law enforcement agencies.[51]

[13] The lines between private and public ALPR operators have begun to blur even further. Although ALPRs are becoming less expensive, each reader can still set police departments back tens of thousands of dollars.[52] As a solution, Vigilant Solutions has rolled out a pilot program that offers these scanners and access to their extensive databases at no cost to police departments.[53] In exchange, the departments give Vigilant Solutions access to information about all individuals with outstanding court costs.[54] The company then sets the system to alert officers to these individuals.[55] When an ALPR gets a *hit* on someone from that list, the suspect is pulled over and offered two options: either get arrested or pay the outstanding court costs plus an additional 25%. That extra 25% goes directly to Vigilant Solutions.[56]

---

[50] *See* Conor Friedersdorf, *An Unprecedented Threat to Privacy*, THE ATLANTIC (Jan. 27, 2016), https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/ [https://perma.cc/SS38-NM6J].

[51] *See id.*; *see also You are Being Tracked*, *supra* note 1.

[52] *See Reduced Prices for License Plates, supra* note 15 (stating that the price of an ALPR system has fallen from an initial cost of $24,000 to $17,000 as of January 2012).

[53] *See* David Maass, *"No Cost" License Plate Readers are Turning Texas Police into Mobile Debt Collectors and Data Miners*, ELECTRONIC FRONTIER FOUND. (Jan. 26, 2016), https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and [https://perma.cc/VS4T-49AY].

[54] *See id.*

[55] *See id.*

[56] *See id.*

[14] Even without Vigilant Solutions concocting novel ways to exploit ALPR databases, police department use of ALPR devices can be problematic. The Virginia State Police highlighted the potential hazards when they used ALPRs to scan plates of all vehicles entering parking lots for Barack Obama and Sarah Palin rallies in 2008.[57] Similarly, Immigrations and Customs Enforcement (ICE) worked with local law enforcement to scan all plates entering lots for a gun show in 2010.[58]

[15] The use of ALPRs at political and social events prompts serious concerns of whether that use chills constitutional rights.[59] The Supreme Court has long recognized that the right to freedom of association may be infringed by requiring private organizations to disclose their membership.[60] The Court has particularly "recognized the vital relationship between [the] freedom to associate and privacy in one's association."[61] The use of ALPRs to automatically and methodically archive individuals' attendance at these events may interfere with this vital relationship.

[16] Apparently ICE's operation of ALPRs has been successful and unchallenged. In 2017, the agency finalized a contract with Vigilant

[57] *See* Letter from Alvin D. Blankenship, First Sergeant, Commonwealth of Va. Dep't of State Police, to Bobbie D. Morris, First Sergeant, Commonwealth of Va. Dep't of State Police (Mar. 18, 2009), http://www.thenewspaper.com/rlc/docs/2013/va-alpr.pdf [https://perma.cc/AXN7-BDVF] (regarding Division Seven Heat Operations.

[58] *See* Devlin Barrett, *Gun-Show Customers' License Plates Come Under Scrutiny*, WALL ST. J. (Oct. 2, 2016, 7:35 PM), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302 [https://perma.cc/5MTT-WUZ7].

[59] *See* Brief for Petitioner at 8, 10, Am. Civil Liberties Union Found. v. Sup. Ct., 400 P.3d 432 (Cal. 2017) (No. S227106) (discussing a public records request for ALPR data with constitutional arguments regarding their use).

[60] *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 458–60 (1958).

[61] *Id*. at 462; *see also* Bates v. City of Little Rock, 361 U.S. 516, 523 (1960).

Solutions to access their database of billions of plate scans.[62] The implications of this contract are unsettling because ICE may be able to use Vigilant Solutions' database to bypass sanctuary city policies.[63] Sanctuary cities are municipalities that, to a certain degree, have decided not to cooperate with federal immigration enforcement.[64] Santa Clara, Contra Costa, Marin, Orange, and San Bernardino counties in California all have sanctuary policies, however, they all also share their ALPR scans with Vigilant Solutions.[65] As a result, ICE's new partnership has the potential to render sanctuary policies essentially useless.

[17] Proponents of unrestricted ALPR use often argue that these databases are only used to catch criminals.[66] The vast majority of data collected and stored in these databases, however, does not correspond to known criminal activity.[67] For example, Maryland's plate reader system captured 29 million scans in 2012.[68] Only 0.2% of those 29 million scans

[62] *See* Alexa Lardieri, *ICE Gets Access to License Plate Recognition, Tracking System*, U.S. NEWS & WORLD REP. (Jan. 26, 2018), https://www.usnews.com/news/politics/articles/2018-01-26/ice-gets-access-to-license-plate-recognition-tracking-system (last visited Mar. 14, 2019).

[63] *See id*.

[64] Stephen Dinan, *Half of all Americans now Live in 'Sanctuaries' Protecting Immigrants*, WASH. TIMES (May 10, 2018), https://www.washingtontimes.com/news/2018/may/10/half-of-americans-now-live-in-sanctuaries/ [https://perma.cc/BDG8-2ALP].

[65] April Glaser, *Sanctuary Cities Are Handing ICE a Map*, SLATE: FUTURE TENSE (Mar. 13, 2018), https://slate.com/technology/2018/03/how-ice-may-be-able-to-access-license-plate-data-from-sanctuary-cities-and-use-it-for-arrests.html [https://perma.cc/EU4P-TEZH].

[66] *See* Shockley, *see supra* note 49.

[67] *See You Are Being Tracked*, *supra* note 1, at 13 (indicating that one percent of license plate reads result in hits on drivers with criminal records).

[68] *See id*.

revealed any potential criminal activity associated with the scanned vehicle or its owner.[69] Furthermore, 97% of the scans that came back with a *hit* only related to suspended licenses or emissions violations.[70] Only 47 out of every one million scans revealed any potential connections to serious crimes.[71]

[18] By plotting vehicle locations at specific times and tracking their movements, ALPRs can be used to paint incredibly detailed portraits of drivers' lives.[72] These scans can be used to determine past behaviors, predict future ones, to solve crimes, or simply to track an individual's movements.[73] As more ALPRs are used, the portraits they paint will likely continue to grow more detailed and invite potential misuse.

III. POTENTIAL OPTIONS TO REGULATE ALPR USE

[19] ALPR regulation is scarce. Only a handful of states have passed any regulations on the industry.[74] A handful more have considered regulations but have declined to pass any.[75] One would assume that ALPRs fall within the scope of Fourth Amendment searches, and thus could be regulated by the federal system. Unfortunately, that is currently not true. Meanwhile, Congress is unwilling to even consider enacting

[69] *See id*.

[70] *See id*.

[71] *See id*. at 14.

[72] *See generally* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (arguing that using GPS to plot vehicle locations can generate a great deal of information about a driver's daily life).

[73] *See id.*

[74] *See generally Automated License Plate Readers: State Statutes*, *supra* note 37 (listing state regulations of ALPRs).

[75] *See infra* section III (c).

federal guidelines.[76] Only two bills on the matter, which would have limited scan data retention to thirty days, have been introduced to Congress; both died in committee.[77] Perhaps Congress is unwilling to delve into the quandary presented by regulating an industry populated by state agencies and private actors working in tandem. It may also be letting the issue percolate through the courts and state legislatures before deciding if federal legislation is truly necessary.

[20] Supreme Court jurisprudence has forced the Fourth Amendment into a corner, from which ALPRs are essentially untouchable.[78] A recent Supreme Court of Virginia decision has potential to outlaw the industry entirely,[79] but this solution strikes an inappropriate balance due to its potential to severely restrict Virginia law enforcement efforts.[80] Virginia's best option is to lobby for narrowly-tailored regulations on ALPRs that will enable their use for criminal justice while minimizing their effects on civil liberties.

[76] *See* Reasonable Policies on Automated License Plate Readers Act, H.R. 4303, 115th Cong. (2017) (failed in committee); Reasonable Policies on Automated License Plate Readers Act, H.R. 2644, 113th Cong. (2013) (same).

[77] *See id*.

[78] *See* United States v. Jones, 565 U.S. 400, 412 (2012); California v. Ciraolo, 476 U.S. 207, 213 (1986); United States v. Karo, 468 U.S. 705, 721 (1984).

[79] *See* Neal v. Fairfax Cty. Police Dep't, 295 Va. 334, 350 (Va. 2018).

[80] *See infra* section III (c); *see also Automated License Plate Readers: State Statutes*, *supra* note 37.

A. ALPR Use Does Not Trigger the Fourth Amendment Because There Is No Expectation of Privacy on Public Roads and the Supreme Court has Declined to Recognize Privacy in One's Long-term Movements

[21] Federal courts have avoided considering the constitutionality of ALPR use.[81] This reluctance to intervene is frustrating.[82] On first glance, ALPRs appear similar to the warrantless GPS tracking that was declared a violation of the Fourth Amendment in *United States v. Jones*.[83] On second glance, they seem ripe for First Amendment challenges; surely the pervasive tracking of individuals as they attend church or political rallies would have unconstitutional chilling effects on the targets' speech and assemblies.

[22] Unfortunately, there has been limited success challenging any level of ALPR use in federal court under either amendment.[84] The Fourth Amendment provides no protection for the basic data collected by ALPRs.[85] Publicly viewable information requires no suspicion on the part

[81] *See* National Association of Criminal Defense Lawyers, *Automated License Plate Readers* (2016) [hereinafter NACDL] (presented information is in the form of a primer which was prepared in partnership with the Samuelson Law, Technology & Public Policy Clinic at UC Berkeley, School of Law).

[82] *See, e.g*., Jessica G. Alm, *The Privacies of Life: Automatic License Plate Recognition Is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127, 156 (2015); *see also* Brian Pascal, *How Technology Broke Privacy*, 40 LITIG. 3, 26 (2014).

[83] *See* United States v. Jones, 565 U.S. 400, 404 (2012).

[84] *See* NACDL, *supra* note 81.

[85] *See* United States v. Diaz-Castaneda, 494 F.3d 1146, 1150 (9th Cir. 2007) (collecting cases) ("every circuit that has considered the issue in a precedential opinion has held that license plate checks do not count as searches under the Fourth Amendment").

of government agents before access.[86] One's location as they traverse down public roads, passing ALPRs attached to police vehicles or traffic poles, is similarly not protected by the Fourth Amendment.[87] In much the same way that individuals do not receive Fourth Amendment protection from being followed by police cars for brief periods of time, protection against this basic level of scan aggregation is unlikely to occur. [88]

[23] The majority opinion in *Jones* is as close as the U.S. Supreme Court has come to indicating that driving on public roads may trigger Fourth Amendment protections from unreasonable government intrusion.[89] The Court held that the warrantless[90] installation and month-long monitoring of a GPS device on the underbelly of a suspect's vehicle was a search in violation of the Fourth Amendment.[91]

[24] Although the overall decision in *Jones* indicates potential for limiting ALPR scans, a closer reading is discouraging. The majority rested its decision not on the length of the monitoring or the private details gleaned from the GPS device, but on the fact that it was installed on the defendant's vehicle while the vehicle was in his possession.[92]

---

[86] *See* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that there is no reasonable expectation of privacy in anything viewable to the naked eye from public space).

[87] *See* United States v. Karo, 468 U.S. 705, 721 (1984).

[88] *See Karo*, 468 U.S. at 721; *see also* United States v. Jones, 565 U.S. 400, 412 (2012).

[89] *See Jones*, 565 U.S. at 404.

[90] Law enforcement obtained a warrant for the installation and monitoring, but it expired the day before they successfully installed the device. This was treated as if no warrant was obtained for the purpose of the Fourth Amendment. *See id*. at 403.

[91] *See id*. at 404.

[92] *See id*. at 404–05.

[25] The Court declared in *Katz v. United States* that the Fourth Amendment protects "people not places."[93] The Court specifically explained that the Fourth Amendment protects people from unreasonable government intrusion when they have a subjective expectation of privacy that the public is willing to accept as objectively reasonable.[94] Under *Jones*, however, the government's trespass on an individual's private property is sufficient to blur the lines between people and places, triggering Fourth Amendment protection. This logic does not rest on the privacy of the information gathered, but rather on the privacy of the individual in their personal, tangible possessions.

[26] The *Jones* majority explicitly had no interest in overturning or amending *U.S. v. Knotts*[95] or *U.S. v. Karo*,[96] which each involved warrantless GPS tracking without the issue of a trespass.[97] In *Knotts*, law enforcement placed a tracking device in a container, gave the container to a suspect, and then monitored his movements with the tracker for three days.[98] The Court found that a person "traveling on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[99] Simply by traveling on public roads, the defendant had waived any Fourth Amendment right to privacy in his location. [100]

[93] Katz v. United States, 389 U.S. 347, 351 (1967).

[94] *See id.* at 361 (Harlan, J., concurring).

[95] *See* United States v. Knotts, 460 U.S. 276, 276 (1983).

[96] *See* United States v. Karo*,* 468 U.S. 705, 705 (1984).

[97] *Compare Katz*, 389 U.S. at 353 (involving a public phone booth), *with Karo*, 468 U.S. at 713 (involving a beeper placed in property given to defendants), *and Knotts*, 460 U.S. at 278 (involving essentially the same situation as in *Karo*).

[98] *See Knotts*, 460 U.S. at 278–79.

[99] *Id*. at 281.

[100] *See id*.

[27] The facts of *Karo* were similar to *Knotts*, but involved the monitoring of a tracking device inside a suspect's home.[101] The Supreme Court drew a line at this particular approach because of the heightened privacy interests in a home—allowing warrantless "monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home."[102] In short, the *Karo* Court simply laid the foundation for the *Jones* ruling that the government's trespass on an individual's personal effects implicates the Fourth Amendment.

[28] *Jones*, *Knotts*, and *Karo* show the unfeasibility of imposing limits on active ALPR use through the Fourth Amendment. As established in *Katz*, individuals only have Fourth Amendment protections when they have a subjective expectation of privacy that society is willing to accept as objectively reasonable.[103] *Karo* imposed protection from tracking in the home, while *Knotts* opened the door to tracking on public roads.[104] Meanwhile, *Jones* reiterated a common law consideration of whether the government somehow trespassed on an individual's private effects when they attempted to gather information, which does not come into play when the governmental action is merely taking pictures of license plates from public roads.[105]

---

[101] *See* United States v. Karo, 468 U.S. 705, 714 (1984); United States v. Knotts, 460 U.S. 276, 278–79 (1983).

[102] *See Karo*, 468 U.S. at 716.

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

[104] *Compare* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that a beeper in a container violates the Fourth Amendment if the container enters an individual's house without the owner's consent), *with* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding a person traveling on a public road has no reasonable expectation of privacy).

[105] ALPRs sometimes capture images of cars actually parked in driveways. This tracking is questionable from a Fourth Amendment perspective but would be unlikely to result in substantive changes to ALPR use. *See* Gil Aegerter, *License Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, NBC NEWS (Nov. 2, 2015, 6:32 PM), https://www.nbcnews.com/news/world/license-plate-data-not-just-cops-private-companies-are-tracking-flna6C10684677 [https://perma.cc/9HFV-Z9NG].

[29] The most encouraging language from the Supreme Court when it comes to Fourth Amendment protections from limitless ALPR scans actually comes from the concurrences in *Jones*.[106] Justices Alito, Ginsburg, Breyer, and Kagan joined in a concurrence that urged the Court to consider not whether the government somehow trespassed on a suspect's property, but whether society is willing to recognize a reasonable expectation of privacy in the long-term monitoring of an individual's vehicle. [107]

[30] This concurrence, had it won the majority vote in *Jones*, would have effectively destroyed the ALPR database industry and forced rapid expiration dates on plate scans.[108] The concurrence did not want to return to the common law consideration of whether a trespass had occurred.[109] It felt that in doing so, the majority was sidestepping the actual problem—the long term monitoring of a suspect's movements. The majority also refused to recognize the technological advances in monitoring that do not require physical trespass, such as cell phone tracking, toll booth cameras, and video monitoring.[110] Alito's approach would have destroyed the passive ALPR industry because it would have eliminated the government's ability to engage in long-term warrantless monitoring of individuals.

[106] *See* United States v. Jones, 565 U.S. 400, 418–19 (2012) (Alito, J., concurring).

[107] *See id.*

[108] *See id.*

[109] *See id*. at 422 (arguing that *Katz* moved beyond the question of whether there had been a trespass, and that the majority was taking a step backwards in its approach to the Fourth Amendment).

[110] *See generally id.* (holding that the *physical* placing of a GPS tracking unit on the defendant's vehicle without a warrant constituted a *search* within the meaning of the Fourth Amendment).

[31] Justice Sotomayor also wrote a concurrence that would have led to Fourth Amendment protection against long-term ALPR tracking.[111] She largely agreed with the Alito concurrence and felt that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[112] She wanted to preserve the common law trespass consideration, however, and thus was split between the majority and Alito opinions.[113]

[32] One unique point in the Sotomayor concurrence was that she appears to agree that long term monitoring could constitute a First Amendment violation by noting that "[a]wareness that the Government may be watching chills associational and expressive freedoms."[114] Indeed, ALPRs and their databases have been used by government agents to implicitly chill First Amendment rights. In 2008, Virginia State Police used ALPRs to scan plates at political rallies.[115] In 1998, a D.C. police officer pled guilty to using an ALPR database to extort people whose cars were scanned outside of a gay nightclub.[116] Although these incidents are few and far between, the incidents make the potential chilling effect of ALPR abuse clear because if people are aware that the government is watching, they may feel compelled to alter their behavior.[117]

---

[111] *See* United States v. Jones, 565 U.S. 400, 414–19 (2012) (Sotomayor, J., concurring).

[112] *See id.* at 415 (Sotomayor, J., concurring) (quoting J. Alito's concurrence).

[113] *See id*. at 414.

[114] *See id*. at 416.

[115] *See* Mark Bowes, *Police Recorded License Plates at Obama Inauguration*, RICHMOND TIMES-DISPATCH (Aug. 18, 2013), https://www.richmond.com/news/local/crime/police-recorded-license-plates-at-obama-inauguration/article_32678a59-f9e1-5e46-8336-d5f4ba076cb7.html [https://perma.cc/4GWB-HT32].

[116] *See* Angwin & Valentino-Devries, *supra* note 15.

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

[33] Unfortunately, most of the litigation around ALPRs involving the First Amendment has come on behalf of the database companies as they have fought against government regulations.[118] The Supreme Court has held that the "creation and dissemination of information are speech within the meaning of the First Amendment."[119] Accordingly, an outright ban on ALPRs, at least in the private sector, would certainly be in violation of the First Amendment as infringing on commercial speech.[120] Use of private databases by government agents does bring the potential of an interesting constitutional issue—how would a court rule between an individual's First Amendment right to assembly versus a private company's right to maintain an unlimited database of ALPR scans?

[34] At this point, the Supreme Court does not appear prepared to declare that ALPR use triggers either the First or Fourth Amendments. The First Amendment jurisprudence is simply not sufficiently developed to draw such a conclusion. The Fourth Amendment jurisprudence, while technically still promising as demonstrated by the *Jones* concurrences, appears to be returning to an approach more focused on trespass and property than the aggregate monitoring of individuals.

B. The Government Data Collection & Disseminations Practice Act Likely Restricts Passive ALPR Use

[35] The constitutionality of long-term ALPR monitoring is an issue that will need more time to develop. In the meantime, the Supreme Court of Virginia recently declared that the storage of ALPR scans in Virginia is likely illegal under the 1976 Government Data Collection &

[118] *See, e.g.*, Digital Recognition Network, Inc. v. Hutchinson, 803 F.3d 952, 954 (8th Cir. 2015); Complaint at 2–3, 16, Digital Recognition Network, Inc. v. Herbert, 803 F.3d 952 (8th Cir. 2015) (No. 2:14-cv-00099-CW) (voluntarily dismissed by plaintiff on April 29, 2014).

[119] Sorrell v. IMS Health, Inc., 564 U.S. 552, 570 (2011).

[120] *See id*.

Dissemination Practices Act (the Act).[121] As a result of this decision, the legislature may need to pass legislation in the near future to clarify permissible uses of passive ALPR data if the practice is to continue in Virginia.[122]

[36] The Act broadly limits the government's ability to collect or store individuals' "personal information" on an "information system" without ongoing criminal investigations.[123] The Act was passed in 1976, well before the proliferation of ALPRs, but was interpreted by most state law enforcement agencies to not include plate scans.[124] The term *personal information* is actually a term of art and that has led to a narrow interpretation of the Act.[125] License plate numbers alone are almost certainly not covered by the Act because they do not reveal any information about an individual.[126] The location of an individual is

[121] *See* VA. CODE ANN. § 2.2-3800–09 (2019); *see also* Neal v. Fairfax Cty. Police Dep't, 295 Va. 334, 350 (2018).

[122] *See* Neal v. Fairfax Cty. Police Dep't, 295 Va. 334,350 (2018).

[123] *See generally* VA. CODE ANN. § 2.2-3801 (2018) (defining "personal information" and "information system" in the Act).

[124] *See* Covington Burlington, *supra* note 41.

[125] *See, e.g.*, Tom Jackman, *Va. Supreme Court to Hear Case Challenging Police Retention of Plate Date,* WASH. POST (June 27, 2017), https://www.washingtonpost.com/news/true-crime/wp/2017/06/27/__trashed-2/?utm_term=.b2c7f5869466 [https://perma.cc/9GXK-DE36].

[126] *See* VA. CODE ANN. § 2.2-3801 (2018) (defining "personal information" in part as including "information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution.").

arguably personal information, but GPS assignments to ALPR scans are merely identifying where an individual's vehicle was located, not necessarily the individual himself.[127] Therefore, agencies in Virginia have felt free to collect and store ALPR scans without regulation.[128]

[37] *Neal v. Fairfax County Police Department* was a relatively straightforward case of statutory interpretation. The plaintiff argued that the Act includes license plate scans, specifically their use in a database to track an individual's long-term movements.[129] He pointed to the sweeping language of the statute as indicating the General Assembly intended the Act to be interpreted broadly.[130] In 2013, then-Attorney General of Virginia, Kenneth Cuccinelli agreed with this interpretation and wrote to the Virginia State Police that routine plate scans without pre-existing suspicion of criminal activity would be barred under the Act.[131] The Virginia State Police has since suspended their ALPR use.[132]

[38] The Fairfax County Police Department disagreed and amici pointed back to cases like *Knotts* that declare there is no privacy—thus, no *personal information*—in one's location on public roads or other publicly

[127] *See id*.

[128] *See, e.g.,* Complaint, Neal v. Fairfax Cty. Police Dep't, 295 Va. 334 (2018) (No. 170247), 2015 WL 2330353.

[129] *See id.* at 2–3.

[130] *See id.* at 4–5.

[131] *See* Advisory Opinion Letter from Kenneth T. Cuccinelli, Op. Va. Att'y Gen., to Colonel W.S. Flaherty, Superintendent Va. Dep't of State Police (Feb. 13, 2013), https://www.thenewspaper.com/rlc/docs/2013/va-stopalpr.pdf [https://perma.cc/DQW4-BFP7].

[132] *See* Rebecca Glenberg, *Virginia State Police Used License Plate Readers at Political Rallies, Built Huge Database*, AM. CIV. LIBERTIES UNION (Oct. 8, 2013, 5:14 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/virginia-state-police-used-license-plate-readers [https://perma.cc/34JQ-86EW].

viewable information.[133] They further argued that even if license plate numbers are somehow personal information, their database should be allowed because it "deal[s] with investigations and intelligence gathering related to criminal activity," a specific exemption from the Act.[134]

[39] In a shocking decision, the Supreme Court of Virginia largely agreed with Neal.[135] The court agreed that individuals' license plate number and location was sufficiently *personal information* under the Act,[136] and it agreed that the criminal activity exemption did not apply because there was no suspicion of criminal activity at the time the scans were conducted. [137]

[40] For the Act to apply, however, the court had to find that the scan databases contained "identifying particulars" from which drivers' identities could be determined.[138] Otherwise, they are not "information systems" as defined by the Act.[139] ALPR scan databases do not, however, contain anything other than images of license plates, dates, times, and locations. Officers in Fairfax County typically must use a separate search engine to locate vehicle owners' names.[140] As a result, the court felt it

[133] *See* Brief for Digital Recognition Network, Inc. et al. as Amici Curiae in Support of Appellees, Neal v. Fairfax Cty. Police Dep't, 295 Va. 334 (2018) (No. 170247), 2017 WL 10441250 at *7.

[134] Brief of Appellees, Neal v. Fairfax Cty. Police Dep't, 295 Va. 334 (2018) (No. 170247), 2017 WL 10441247, at *14 (quoting VA. CODE ANN. § 2.2-3802(7)).

[135] *See* Neal v. Fairfax Cty. Police Dep't, 295 Va. 334, 350 (2018).

[136] *See id*. at 346–47.

[137] *See id*. at 348–50.

[138] *See id*. at 348–49.

[139] *See id*.

[140] *See* Neal v. Fairfax Cty. Police Dep't, 295 Va. 334, 348–49 (2018). *But see License Plate Reader Technology supra* note 7 (discussing other departments' use of NCIC to

could not decide whether the database truly contained "identifying particulars" and remanded the case to Fairfax County Circuit Court.[141] The Fairfax County Circuit Court must decide whether a database that requires the use of another database to identify an individual is covered by the Act.[142] If so, and the higher courts agree, passive ALPR use in Virginia will essentially be banned.[143]

C. A Mixture of Legislation and Internal Policy Is the Best Option to Balance Government and Public Interests

[41] The ultimate result desired by the appellant in *Neal,* an outright ban on passive ALPR use, does not seem necessary because the minimal intrusion performed by ALPRs may be acceptable with proper regulation.[144] Barring the passive use of ALPRs would be the strictest regulation in the nation. A handful of states have passed regulations on ALPRs that have proven effective at minimizing opportunities for abuse

automatically connect ALPR scans to intensive background checks on the vehicle's owners).

[141] *See Neal*, 295 Va. at 347, 350.

[142] *See id.* at 350.

[143] The Fairfax County Circuit Court issued a letter opinion in *Neal* on April 1, 2019. *See* Neal v. Fairfax Cty. Police Dep't, No. CL-2015-5902 (Va. Cir. Ct. 19th Apr. 1, 2019) https://www.fairfaxcounty.gov/circuit/sites/circuit/files/assets/documents/pdf/opinions/cl-2015-5902-neal-v-fcpd-et-al-2.pdf [https://perma.cc/KC3J-GKMV]. The court found that ALPR use "provides a means through which a link to the identity of a vehicle's owner can be readily made," and therefore violates the Data Act. *Id.* at 5; *see also* Tom Jackman, *Judge Orders Fairfax Police to Stop Collecting Data from License Plate Readers*, WASH. POST (Apr. 2, 2019), https://www.washingtonpost.com/crime-law/2019/04/02/judge-orders-fairfax-police-stop-collecting-data-license-plate-readers/?utm_term=.9108e7c38382 [https://perma.cc/4E9N-4RMS].

[144] *See* David J. Roberts & Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement*, U.S. DEP'T JUST. 35 (Sept. 2012), https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf [https://perma.cc/YW75-DDQ6] (advocating for responsible policies to restrict the use of passive ALPR use without an outright ban on the practice).

while preserving the devices' investigative capacities.[145] This is the middle ground for policy change that has already shown promise in the Virginia legislature.

[42] In 2015, the General Assembly passed legislation that would have required government agencies to delete license plate scans within seven days.[146] However, law enforcement officers heavily opposed this bill and pointed to how scans had been used to locate missing persons and prisoners in Virginia.[147] Then-Governor McAuliffe responded to law enforcement concerns by demanding that the deadline be extended to two months.[148] When the legislature declined his amendment, he vetoed the bill, leaving Virginia without regulations on plate readers.[149]

[43] As visualized below in Table 1, the Virginia legislature's proposed seven-day deadline is quite strict when compared to similar laws around the country. Even Governor McAuliffe's 60-day deadline would have been stricter than most. These deadlines are generally waived if the scans are part of an ongoing criminal investigation, allowing departments to hold scans indefinitely.[150]

[145] *See generally id.* (discussing which states have passed ALPR statutes and what those statutes contain).

[146] *See* Jenna Portnoy & Tom Jackman, *McAuliffe Vetoes Surveillance Technology Bill to Chagrin of Privacy Hawks*, WASH. POST (May 1, 2015), https://www.washingtonpost.com/local/virginia-politics/mcauliffe-vetoes-surveillance-technology-bill-to-chagrin-of-privacy-hawks/2015/05/01/8c4fe46c-ef57-11e4-8666-a1d756d0218e_story.html?utm_term=.b25f62f7d8cc [https://perma.cc/KKM3-JUR5].

[147] *See id.*

[148] *See id.*

[149] *See id.*

[150] *See infra* Table 1.

Table 1

Legislatively Imposed Retention Policies	
State	**Deletion Deadline**
New York	Inconclusive[151]
New Jersey	5 years[152]
Colorado	3 years[153]
Florida	3 years[154]
Georgia	30 months[155]
Vermont	18 months[156]

[151] *See* N.Y. STATE DIV. CRIMINAL JUSTICE SERVS., SUGGESTED GUIDELINES: OPERATION OF LICENSE PLATE READY TECHNOLOGY 10 (2011) (recommending each department come up with its own retention policies); *see also* Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime as well as Terrorism*, REUTERS (June 21, 2013, 11:24 AM), https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSL2N0EV0D220130621 [https://perma.cc/L958-R93Q] (stating that NYPD reportedly retains scans for up to five years).

[152] *See* Paula T. Dow, *Directive No. 2010-5*, STATE OF N.J.: OFFICE OF ATTORNEY GENERAL 7 (2010), https://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf [https://perma.cc/V82B-YDVY].

[153] *See* COLO. REV. STAT. § 24-72-113 (2014) (restricting use after one year since date of collection).

[154] *See* State of Florida, Criminal and Juvenile Justice Information Systems Council, *Guidelines for the Use of Automated License Plate Readers*, https://www.fdle.state.fl.us/CJJIS/Documents/CJJIS-Council-ALPR-Guidelines [https://perma.cc/2TLX-H6XK].

[155] *See* GA. CODE ANN. § 35-1-22(b) (2018).

[156] See VT. STAT. ANN. tit. 23, § 1607(d)(2) (2018).

Utah	9 months[157]
Arkansas	150 days[158]
North Carolina	90 days[159]
Montana	90 days[160]
Tennessee	90 days[161]
California	60 days[162]
Minnesota	60 days[163]
Maine	21 days[164]
New Hampshire	3 minutes[165]

[157] *See* UTAH CODE ANN. § 41-6a-2004(1)(c) (2018).

[158] *See* ARK. CODE ANN. § 12-12-1804(a) (2018).

[159] *See* N.C. GEN. STAT. § 20-183.32(a) (2018).

[160] *See* MONT. CODE ANN. § 46-5-118(1) (2017).

[161] *See* TENN. CODE ANN. § 55-10-302(4) (2019).

[162] *See* CAL. VEH. CODE § 2413(b) (West 2018) (restricting specifically California Highway Patrol and only for scans not used in felony cases).

[163] *See* MINN. STAT. ANN. § 13.824(3)(a) (West 2018).

[164] *See* ME. REV. STAT. ANN. tit. 29, § 2117-A(5) (2018).

[165] *See* N.H. REV. STAT. ANN. § 261:75-b(VIII) (2018).

[44] In addition to legislatively imposed retention policies, many law enforcement agencies have internal policies to delete their scans within a reasonable length of time. For example, although Minnesota State Patrol has only a 0.5% successful hit rate on ALPR scans, it does not place its non-hit scans into a database at all.[166] Instead, it has imposed an internal policy that all scans must be deleted within forty-eight hours unless there are "extenuating circumstances."[167] As a result, on any given day it is unlikely that the agency stores more than 20,000 ALPR scans.[168]

[45] As shown below in Table 2, a combination of FOIA requests and a 2012 study of police departments in Northern Virginia reveal that departments are willing to impose relatively strict retention policies. These policies typically include an exception if the scan is needed for legitimate law enforcement purposes.[169] A relatively loose deadline for deletion of ALPR data set by the legislature could create a "hard ceiling" for policies, while leaving most agencies free to follow their current internal guidelines.

[166] *See You Are Being Tracked*, *supra* note 1, at 15.

[167] *See id.*, at 16 (citations omitted); *see also* Minnesota State Patrol, *General Order on License Plate Readers* (Sept. 28, 2009), https://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(3).pdf [https://perma.cc/X5ZE-XSYK].

[168] *See You Are Being Tracked*, *supra* note 1, at 17–18.

[169] *See* Brief of Appellees at 14–18, Neal v. Fairfax Cty. Police Dep't, 295 Va. 334 (2018) (No. 170247), 2017 WL 10441247.

Table 2

Internally Imposed Retention Policies (VA)	
Police Department	**Deletion Deadline**
Fairfax County	1 year[170]
Alexandria City	2 years[171]
Norfolk City	Held for at least 30 days, then deleted "according to manufacturer's specifications"[172]
Prince William County	30-60 days[173]
Arlington County	30 days[174]
Virginia State Police	24 hours[175]

[170] *See* Brief of Appellant at 7, Neal v. Fairfax Cty. Police Dep't, 295 Va. 334 (2018) (No. 170247), 2017 WL 10441246. Although Fairfax's official deletion deadline is one year, scans have been retained for two years due to computer errors.

[171] *See* Allison Klein & Josh White, *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns*, WASH. POST (Nov. 19, 2011), https://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html?utm_term=.9de2784adec9 [https://perma.cc/N5WL-3C4J].

[172] *See* City of Norfolk, *Operational General Order–492* (May 31, 2012), https://www.muckrock.com/foi/norfolk-county-414/automated-license-plate-reader-alpr-adoption-use-and-data-retention-policies-norfolk-police-department-65996/#file-763950 [https://perma.cc/E7QS-8MDJ].

[173] *See* Graphic: Who Has LPR Cameras and How Long Do Police Hold on to Information?, WASH. POST (Nov. 5, 2011), https://www.washingtonpost.com/local/2011/11/05/gIQAoWGdqM_graphic.html?utm_term=.a65f3028d7c1 [https://perma.cc/U9ET-J2G7].

[174] *See id*.

[46] The broad range of internal deletion policies in these Virginia departments is troubling. Without a statewide deadline, officers in Arlington may use scans significantly in excess of their thirty-day deadline from neighboring Alexandria to compile cases. A legislatively imposed sixty-day state deadline as advocated for by Governor McAulliffe[176] would force Fairfax and Alexandria police departments to be more reasonable with their retention policies, while allowing departments like Prince William, Arlington, and Virginia State Police the freedom to retain their own stricter policies.

IV. CONCLUSION

[47] For better or for worse, ALPRs have had a significant impact on the ability of private and public actors to track individuals. The active use of these readers can solve crimes in mere seconds. The passive use of these readers and their data, however, has potential to erode constitutional freedoms. On a federal level, ALPR use is unlikely to be regulated in the near future. On a state level, however, several promising options exist. In Virginia specifically, the ultimate outcome of *Neal* may result in ALPRs disappearing from law enforcement hands entirely. As several states have demonstrated through well-tailored regulations on ALPRs, however, such an outcome is unnecessary. Virginia, through its own legislature, can and should strive to reap the benefits of instantaneous background checks and data collection offered by ALPRs while keeping a close eye on protecting constitutional freedoms.

[175] *See* Portnoy & Jackman, *supra* footnote 147.

[176] *See id.*