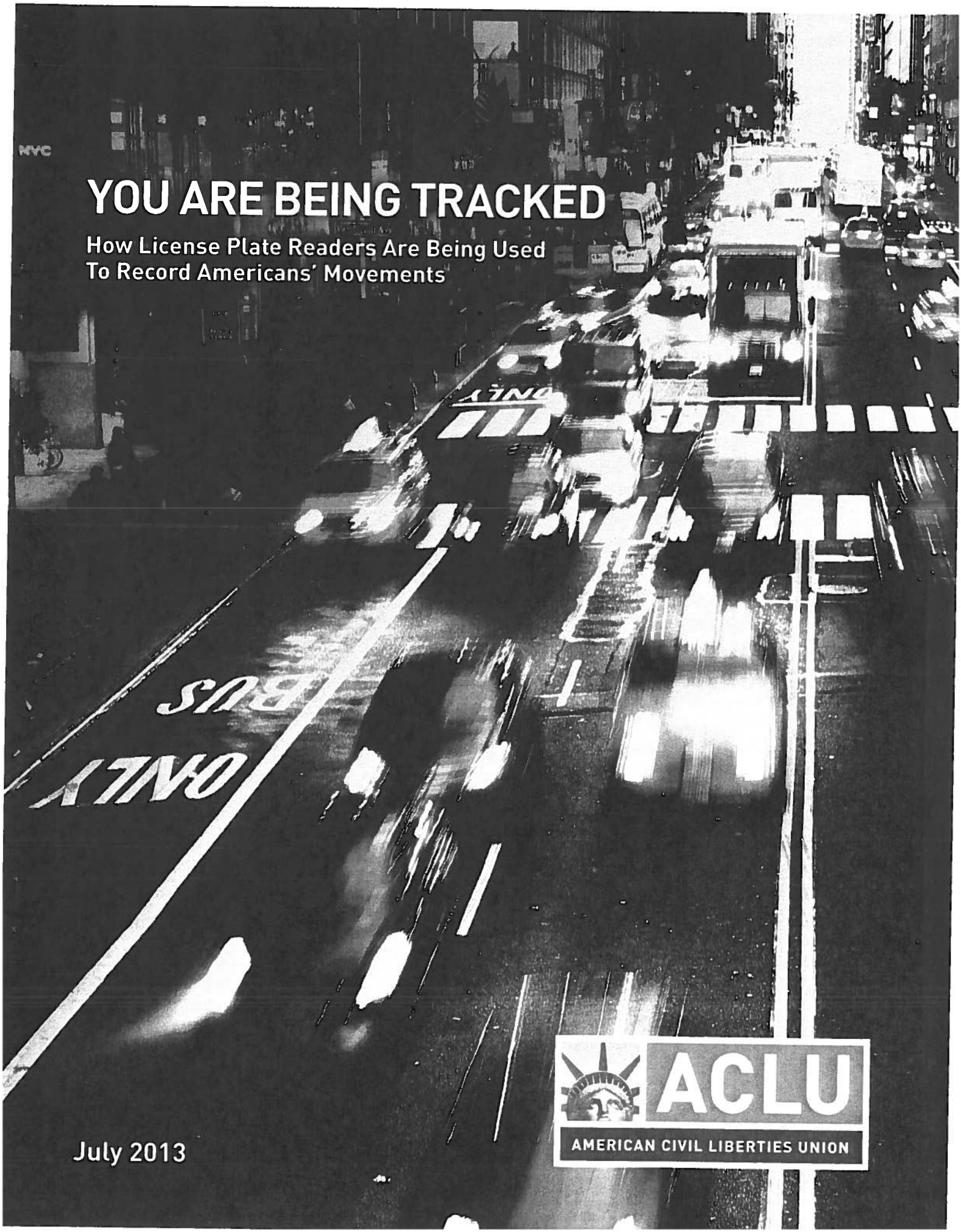
YOU ARE BEING TRACKED

How License Plate Readers Are Being Used To Record Americans' Movements



ACLU

AMERICAN CIVIL LIBERTIES UNION

July 2013

You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements

July 2013

American Civil Liberties Union
125 Broad Street
New York, NY 10004
www.aclu.org

Cover Photo: Newsbound/AP

Table of Contents

INTRODUCTION 2

THE TECHNOLOGY 4

LICENSE PLATE READERS POSE PRIVACY RISKS 7

Chilling effects 7

Abusive tracking 8

Institutional abuse 9

Discriminatory targeting 9

Sidebar: Pervasive, Permanent Monitoring 10

LICENSE PLATE READERS ARE WIDELY USED BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES 12

License plate readers collect vast quantities of data on innocent people 13

Many agencies retain data on innocent Americans for long periods of time 16

All the pieces are lining up for widespread sharing of license plate reader data . . 18

Sidebar: Pushing Back on Invasive License Plate Reader Use: A Success Story . . 23

THE FEDERAL GOVERNMENT IS FUELING STATE AND LOCAL USE OF LICENSE PLATE READERS 25

TOO LITTLE IS KNOWN ABOUT THE FEDERAL GOVERNMENT'S OWN USE OF LICENSE PLATE READERS 27

PRIVATE COMPANIES COLLECT LICENSE PLATE DATA WITH NO OVERSIGHT 28

Sidebar: Data Mining License Plate Records 30

THERE ARE TOO FEW RULES IN PLACE TO PROTECT PRIVACY 31

RECOMMENDATIONS 32

ACKNOWLEDGMENTS 34

INTRODUCTION

If you've never seen an automatic license plate reader, it's probably because you didn't know what to look for. The devices have been proliferating around the country at worrying speed. Mounted on patrol cars or placed on bridges or overpasses, license plate readers combine high-speed cameras that capture photographs of every passing license plate with software that analyzes those photographs to identify the plate number. License plate reader systems typically check each plate number against "hot lists" of plates that have been uploaded to the system and provide an instant alert to a law enforcement agent when a match or "hit" appears.

License plate readers would pose few civil liberties risks if they only checked plates against hot lists and these hot lists were implemented soundly. But these systems are configured to store the photograph, the license plate number, and the date, time, and location where *all* vehicles are seen — not just the data of vehicles that generate hits. All of this information is being placed into databases, and is sometimes pooled into regional sharing systems. As a result, enormous databases of motorists' location information are being created. All too frequently, these data are retained permanently and shared widely with few or no restrictions on how they can be used.

The implementation of automatic license plate readers poses serious privacy and other civil liberties threats. More and more cameras, longer retention periods, and widespread sharing allow law enforcement agents to assemble the individual puzzle pieces of where we have been over time into a single, high-resolution image of our lives. The knowledge that one is subject to constant monitoring can chill the exercise of our cherished rights to free speech and association. Databases of license plate reader information create opportunities for institutional abuse, such as using them to identify protest attendees merely because these individuals have exercised their First Amendment-protected right to free speech. If not properly secured, license plate reader databases open the door to abusive tracking, enabling anyone with access to pry into the lives of his boss, his ex-wife, or his romantic, political, or workplace rivals.

In July 2012, American Civil Liberties Union affiliates in 38 states and Washington, D.C., sent 587 public records act requests to local police departments and state agencies to obtain information on how these agencies use license plate readers. We also filed requests with the U.S. Departments of Justice, Homeland Security, and Transportation to learn how the federal government has used grants to encourage the widespread adoption of license plate readers, as well as how it is using the technology itself.

NUMBER OF POLICE DEPARTMENTS AND STATE AGENCIES WE ASKED FOR RECORDS	NUMBER THAT HAVE RESPONDED SO FAR	NUMBER THAT HAVE NOT RESPONDED
587	293	294

We received over 26,000 pages of documents from the law enforcement agencies that responded to our requests, about their policies, procedures, and practices for using license plate readers.

This report provides an overview of what we have learned about license plate readers: what their capabilities are, how they are being used, and why they raise privacy issues of critical importance. We close by offering specific recommendations designed to allow law enforcement agencies to use license plate readers for legitimate purposes without subjecting Americans to the permanent recording of their every movement.

The potential privacy harms discussed in this report are not merely theoretical. In August 2012, the Minneapolis Star Tribune published a map displaying the location, obtained via a public records request, of the 41 times that Mayor R.T. Rybak's car had been recorded by a license plate reader in the preceding year.[1] The Star Tribune also reported that of the 805,000 plate scans made in June, less than one percent were hits.[2] Yet for as long as the information was retained, the other 99 percent of scans were also vulnerable to the risk that they might be released, used by the police to track innocent people, or otherwise abused. The alarming fact that a law-abiding citizen's sensitive location history could be revealed so easily was not lost on this exposed mayor. In response to the Star Tribune's reporting, he directed the city's chief of police to recommend a new policy on data retention.[3] We hope the findings of our report spur similar policy changes.

---

1 Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, Minneapolis Star Tribune (Aug. 17, 2012), http://www.startribune.com/local/minneapolis/166494646.html.

2 Eric Roper, *Police Cameras Quietly Capture License Plates, Collect Data*, Minneapolis Star Tribune (Aug. 10, 2012), http://www.startribune.com/local/minneapolis/165680946.html.

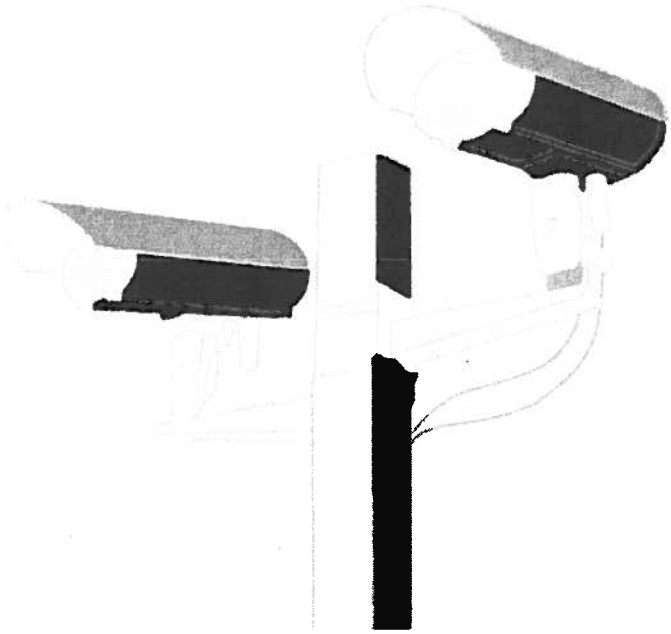
3 *Id.* Minnesota now has a temporary data classification that makes the plate data collected by readers exempt from disclosure under the state public records laws. That temporary classification applies statewide and is set to expire August 1, 2015 absent legislative action on the issue. Minnesota Department of Administration, Information and Analysis Division, *Current Temporary Classifications*, http://www.ipad.state.mn.us/docs/tccurrent.html.

THE TECHNOLOGY

Automatic license plate readers are made up of high-speed cameras designed to capture a photograph of each and every passing license plate, combined with software that analyzes those photographs to identify the license plate number.[4] These systems store extensive location information about each automobile.[5]

License plate reader cameras can be placed almost anywhere, from mobile vehicles like patrol cars[6] to fixed objects like bridges and overpasses.[7] There are even apps that allow law enforcement agents on foot to scan license plates with their smartphones.[8] On taking a photograph, license plate reader systems quickly:

- Identify any license plates within the photograph
- Convert each license plate number into machine-readable text



4 ELSAG North America, Mobile Plate Hunter-900 Car Systems User Guide (June 2011), Documents Received in Response to ACLU Public Records Requests, all of which are available at aclu.org [hereinafter "Public Records Responses"], p. 6422, http://www.aclu.org/files/FilesPDFs/ALPR/vermont/alprpra_departmentofpublicsafety_VT%20(2).pdf; Motorola, Automatic License Plate Recognition Solutions Brief (2011), Public Records Responses p.10717, http://www.aclu.org/files/FilesPDFs/ALPR/illinois/alprpra_burbankpd_burbankil.PDF.

5 L-3 Mobile-Vision, AlertVU Mobile User Manual, Public Records Responses, p. 18733, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/18731-18763%20Woodbridge%20ALPR%20User%20Manual.pdf; Federal Signal, PAGIS ALPR Software Data Sheet (2010), Public Records Responses, p. 18538, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/18537-18538%20Vineland%20OPRA%20Response%2024.pdf; Vigilant Video, Mobile License Plate Recognition Systems, Public Records Responses, p. 15935, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_yonkerspolicedepartment_yonkersny_1.pdf.

6 Federal Signal, Slate ALPR Camera Data Sheet (2009), Public Records Responses, pp. 1866-87, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_AustinPD_AustinTX%20(56).pdf; ELSAG North America, How the MPH-900 Works, (Sept. 16, 2011), Public Records Responses, p. 4334, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_wrightsvillebeachpd_wrightsvillebeachnc%20(3).pdf.

7 Federal Signal, Spike+ Model P372 Data Sheet (2008), Public Records Responses, pp. 2425-26, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_grapevinePD_grapevineTX%20(5).pdf; ELSAG North America, Fixed Plate Hunter-900 (Sept. 16, 2011), Public Records Responses, p. 4330, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_wrightsvillebeachpd_wrightsvillebeachnc%20(3).pdf%20; Prime Communications, Corporate Overview, Public Records Responses, p. 3555, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf.

8 Vigilant Video, CarDetector Mobile Companion, p. 1 (2012(, http://vigilantsolutions.com/wp-content/uploads/2012/09/Vigilant-Mobile-Companion-Datasheet-092012.pdf.

- Check each license plate number against manually entered plate numbers and "hot lists" of plates that have been uploaded to the system
- Provide an instant alert to a law enforcement agent when a match or hit appears
- Store the photograph, the license plate number, and the date, time, and location where the automobile was seen[9]

Prices for license plate reader systems have decreased markedly in recent years and are continuing to fall.[10] State and federal grants can further lower the cost law enforcement agencies must pay out of pocket to purchase license plate reading equipment.[11] The cost of storing data collected from license plate readers is also dropping. Between 2000 and 2010, the inflation-adjusted cost to purchase one gigabyte of hard drive storage fell from about $10 to less than ten cents.[12]

As license plate readers become increasingly widespread, they are being put to a variety of uses. Perhaps the most common law enforcement use of license plate readers is, as described above, to check plates against "hot lists," including the National Crime Information Center vehicle file (which includes stolen vehicles and vehicles used in the commission of a crime). Other common hot lists include the plate numbers of those who are the subject of an AMBER Alert or felony arrest warrant, and people who have been required to register as sex offenders or are on supervised release.[13]

Data collected from license plate readers can also be pooled in centralized databases.[14] Software can then be used to plot all of the plate reads associated with a particular vehicle to trace a person's past movements.[15] The systems can also plot all vehicles at

---

9 Federal Signal, PAGIS ALPR Software Data Sheet (2010), Public Records Responses, pp. 18537-38, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/18537-18538%20Vineland%20OPRA%20Response%2024.pdf; Vigilant Video, National Vehicle Location Service, Public Records Responses, pp. 15939-41, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_yonkerspolicedepartment_yonkersny_1.pdf.

10 According to the Wall Street Journal, the price of a standard two-camera license plate recognition system has dropped from $25,000 to $15,000 in just a few years. Julia Angwin & Jennifer Valentino-Devries, New Tracking Frontier: Your License Plates, Wall St. J. (Sept. 29. 2012), http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html. *See also* Homeland Security News Wire, *Reduced Prices for License Plates [sic] Readers Attracts More Buyers*, (Jan. 24, 2012), http://www.homelandsecuritynewswire.com/srlet20120124-reduced-prices-for-license-plates-readers-attracts-more-buyers (stating that the price of an ALPR system has fallen from an initial cost of $24,000 to $17,000 as of January 2012).

11 ELSAG North America, Grant Guide, http://elsag.com/grant_guide.htm.

12 John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Center For Technology Innovation at Brookings, p. 4 (Dec. 14, 2011), http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf.

13 Federal Signal, PAGIS ALPR Software Data Sheet (2010), Public Records Responses, p. 18537, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/18537-18538%20Vineland%20OPRA%20Response%2024.pdf; High Point Police Department General Order on Automated License Plate Readers (June 1, 2011), Public Records Responses, pp. 812-13, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_HighPointPD_HighPointNC%20(3).pdf.

14 Motorola, Automatic License Plate Recognition Solutions Brief, p. 3 (2011), http://www.motorola.com/web/Business/_Documents/Application%20Briefs/Motorola_ALPR_RO-14-2005B.pdf.

15 *Id.*; Prime Communications, Corporate Overview, Public Records Responses, p. 3557, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf.

a particular location, such as the location where a crime — or a political protest — took place.[16]

Additional uses for license plate readers are arising as the cameras become more affordable and widespread.

VEHICLE VERIFICATION

Photographs captured by license plate readers may contain more than simply the license plate, and sometimes include a substantial part of a vehicle, its occupants, and its immediate vicinity.[17] Law enforcement can use captured photographs to verify witness descriptions of vehicles and confirm identifying features.[18] Photographs of cars and drivers can also be printed and distributed to the press and public.[19]

GEOFENCING

Law enforcement or private companies can construct a virtual fence around a designated geographical area, to identify each vehicle entering that space.[20]

NON-LAW ENFORCEMENT

License plate readers can also be used for non-law enforcement purposes, such as repossession of vehicles and parking enforcement.[21]

---

16 Prime Communications, Corporate Overview, Public Records Responses, p. 3557, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf; Maryland State Police, General Order on Automated License Plate Recognition Program (May 2, 2012), Public Records Responses, p. 502, http://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpramspmd (2).pdf; Miami-Dade Police, Technical Specifications for Mobile License Plate Readers, Public Records Responses, p. 6252, http://www.aclu.org/files/FilesPDFs/ALPR/florida/alprpra_miamidadecountypd_miamicountyfl.pdf.

17 Photographs captured by license plate readers may contain more than simply the license plate. A large manufacturer, ELSAG North America, advertises that its cameras "capture nearly twice the physical area — the sweet spot — and that means more information for law enforcement." The advertised "sweet spot" captures not only the car's license plate, but "a significant portion of the car and part of the car's surroundings," leaving room for the car's driver, the vehicle's passengers, or passing pedestrians to also be captured by the camera. Thus, photographs of individuals are also being captured and stored. ELSAG North America, ALPR Products and Solutions — Mobile Plate Hunter-900, http://www.elsag.com/mobile.htm; International Association of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers, Public Records Responses, pp. 380-81, https://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_MPIA_md.pdf; Prime Communications, Corporate Overview, Public Records Responses, p. 3556, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf; *see generally* Angwin & Valentino-Devries, *supra* note 10.

18 Prime Communications, Corporate Overview, Public Records Responses, p. 3556, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf.

19 *Id.*

20 For example, Tiburon, California has license plate readers monitoring its only two roads that leave the town. Cyrus Favriar, *Rich California Town Considers License Plate Readers For Entire City Limits*, Ars Technica (Mar. 5, 2013), http://arstechnica.com/tech-policy/2013/03/rich-california-town-considers-license-plate-readers-for-entire-city-limits/. Prime Communications, Corporate Overview, Public Records Responses, p. 3557, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf; ELSAG North America, Geofencing Capabilities of the Mobile Plate Hunter-900, p. 1 (Sept. 14, 2011), http://elsag.com/media/content/ELSAG_geofencing-ss(1).pdf.

21 Texas Tech University Parking Service, Parking in the Buff: Parking in a Post-Permit World (Apr. 24, 2012), Public Records Responses, p. 3496-3546, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx (2).pdf; Vigilant Video, National Vehicle Location Services Information Sheet, Public Records Responses, p. 15921, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_yonkerspolicedepartment_yonkersny_1.pdf; Prime Communications, Corporate Overview, Public Records Responses, p. 3555, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_texastechuniversity_lubbocktx%20(4).pdf; Michael Harlow, *License Plate Recognition: It's Grown Far Beyond Airports*, Parking Today (July 2009), http://www.parkingtoday.com/articledetails.php?id=788; Martha Groves, *Servant or Snoop in the Parking Garage?*, L.A. Times (Jan. 23, 2011), http://articles.latimes.com/2011/jan/23/local/la-me-santa-monica-parking-20110123; Angwin & Valentino-Devries, *supra* note 10; Digital Recognition Network, http://www.drndata.com/index.html.

LICENSE PLATE READERS POSE PRIVACY RISKS

Tens of thousands of license plate readers are now deployed throughout the United States. Unfortunately, license plate readers are typically programmed to retain the location information and photograph of *every vehicle* that crosses their path, not simply those that generate a hit.[22] The photographs and all other associated information are then retained in a database, and can be shared with others, such as law enforcement agencies, fusion centers, and private companies.[23] Together these databases contain hundreds of millions of data points revealing the travel histories of millions of motorists who have committed no crime.

Longer retention periods and more widespread sharing allow law enforcement agents to assemble the individual puzzle pieces of where we have been over time into a single, high-resolution image of our lives. This constant monitoring and permanent recording violates our privacy in a number of respects.

Chilling effects

In many places in America, license plate readers were initially deployed relatively sparsely, for example, at the entry and exit points of various towns.[24] But as license plate readers have proliferated, they no longer capture individuals' movements at only a few points. Increasingly, they are capturing drivers' locations outside church, the doctor's office, and school, giving law enforcement and private companies that run the largest databases the ability to build detailed pictures of our lives.

Location data can reveal extremely sensitive information about who we are and what we

22 ELSAG North America, Car System User's Guide (June 2011), Public Records Responses, p. 6422-23, http://www.aclu.org/files/FilesPDFs/ALPR/vermont/alprpra_departmentofpublicsafety_VT(2).pdf; L-3 Mobile-Vision, AlertVU Mobile User Manual, Public Records Responses, p. 18733, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/18731-18763%20Woodbridge%20ALPR%20User%20Manual.pdf.

23 Motorola Solutions Brief, *supra* note 4. *See also* Commerce City, Grant Application to Colorado Automobile Theft Prevention Authority Grant Program (Feb. 1, 2012), Public Records Responses, p. 7881, http://www.aclu.org/files/FilesPDFs/ALPR/colorado/alprpra_commercecitypd_commercecityca (5).pdf (police departments sharing license plate data with each other); Memorandum of Understanding between National Capital Region's License Plate Reader Information Sharing Program and Rockville Police (Mar. 29, 2012), Public Records Responses, pp. 393-99, https://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_MPIA_md.pdf (police department sharing license plate data with a regional fusion center); Vigilant Solutions, Car Detector Mobile ALPR/ANPR (2012), Public Records Responses, p. 15918, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_yonkerspolicedepartment_yonkersny_1.pdf (police departments sharing data with a private company).

24 Tiburon, California takes this approach, and retains data for 30 days. Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, Ars Technica (Sept. 27, 2012), http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/.

do. As the U.S. Court of Appeals for the D.C. Circuit explained in a recent GPS tracking case:

> 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.[25]

And license plate readers can be used for tracking people's movements for months or years on end, chilling the exercise of our cherished rights to free speech and association.

While police departments and government agencies argue that the data they collect will be used only for proper purposes, even the International Association of Chiefs of Police has recognized that pervasive surveillance can have negative chilling effects regardless of its purpose. As it has explained, "The risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[26] Psychologists have confirmed through multiple studies that people do in fact alter their behavior when they know they are being watched.[27] In one such study, the mere presence of a poster of staring human eyes was enough to significantly change the participants' behavior.[28]

Abusive tracking

When police departments lack policies limiting access to license plate data and monitoring its use, abuse of the technology can occur. Other location tracking technologies, such as attachment of GPS devices to vehicles and tracking people

---

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

26 International Association of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, p. 13 (2009), http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87.

27 *See* Jay Stanley, *Does Surveillance Affect Us Even When We Can't Confirm We're Being Watched? Lessons From Behind the Iron Curtain*, Free Future (Oct. 15, 2012), http://www.aclu.org/blog/national-security/does-surveillance-affect-us-even-when-we-cant-confirm-were-being-watched.

28 Sander van der Linden, *How the Illusion of Being Observed Can Make You a Better Person*, Sci. Am. (May 3, 2011), http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person; M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 Penn St. L. Rev. p. 809 (2010), http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf.

through their cell phones, are now regularly utilized to facilitate stalking.[29] There is no reason to believe that license plate readers will prove an exception.

License plate reader systems allow law enforcement agents to enter license plate numbers manually and then receive automated alerts on those plates in the same way they would any plate listed in an approved hot list. This method enables misuse: Anyone with access to these systems could track his boss, his ex-wife, his romantic or workplace rivals, friends, enemies, neighbors, family, and so forth. An agent could target the owners of vehicles parked at political meetings, gay bars, gun stores, or abortion clinics.

Institutional abuse

In addition to abuse by individual law enforcement agents, license plate readers can be subject to larger-scale institutional abuse as a matter of policy. For decades of the 20th century, the FBI and other federal agencies illegally targeted activists in the civil rights, anti-war, and labor movements. Today, law enforcement agencies are again carrying out systematic surveillance of peaceful political protesters.[30] And in other countries, political protesters have already been subjected to surveillance through license plate reader systems. In the United Kingdom, John Catt, a retiree and anti-war protester, was pulled over by an anti-terror unit based on a license plate reader hit.[31] The BBC reports that his license plate was put on a hot list after an anti-war protest.[32]

Discriminatory targeting

License plate reader systems can also facilitate discriminatory targeting. An agent who manually enters plates into a license plate reader system based on discriminatory rationales could check far more plates than he could without the technology. Also, discrimination can exist in deciding where to place the cameras. Whole communities may be targeted based on their religious, ethnic, or associational makeup. In the U.K., law enforcement agents installed over 200 cameras and license plate readers

---

29 Katrina Baum et al., Bureau of Justice Statistics: Stalking Victimization in the United States, at 5 (Jan. 2009) ("Global positioning system (GPS) technology comprised about a tenth of the electronic monitoring of stalking victims."), http://www.ovw.usdoj.gov/docs/stalking-victimization.pdf; Justin Scheck, *Stalkers Exploit Cellphone GPS*, Wall St. J., Aug. 4, 2010, http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html.

30 See ACLU, Spyfiles, www.aclu.org/spyfiles.

31 Richard Bilton, *Camera Grid to Log License Plates*, BBC (May 22, 2009), http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8064333.stm.

32 *Id.*

PERVASIVE, PERMANENT MONITORING

If regulations are not put in place to limit the use of license plate readers, there is a risk that they will be abused through scenarios such as these:

- A citizen group organizes a protest calling for an end to the "war on terror." Many people show up. The police department uses a license plate reader-equipped police cruiser to scan the license plates of all who park in a nearby parking lot to attend the protest. They then investigate these individuals, showing up at their places of employment to ask questions about their backgrounds.

- A journalist at a small newspaper publishes a series of explosive stories charging local police officers with planting drugs on suspects in order to meet arrest quotas. The stories are clearly based on insider information, so police officials park a license plate reader outside the newspaper's office and check each car that drives by against a list of police officers' license plate numbers. When they see an officer paying visits to the newspaper, they fire him on a technicality.

- The mayor of a medium-sized Midwest city is attempting to fight off the first major challenge to his position in over 20 years, and hears a rumor that his challenger has a mistress. He asks his police commissioner to analyze historical license plate reader data for his challenger's license plate, and is able to confirm that he regularly visits the home of a young, single woman after 10 p.m. The mayor anonymously tips off a local journalist, who confirms the affair and publishes a front-page story exposing it.

in predominantly Muslim suburbs of Birmingham.[33] Public outrage was such that the agents dismantled the cameras, stating that cultivating the trust of the community was the more effective approach.[34] In New York City, police officers have reportedly driven unmarked vehicles equipped with license plate readers around local mosques in order to record each attendee.[35] Police departments in other parts of the country could easily do the same thing to Tea Party groups, anti-abortion protesters, or the political opposition of a sheriff running for re-election.

33 Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, The Guardian (Oct. 25, 2010), http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance.
34 *Id.*
35 Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), http://www.ap.org/Content/AP-In-The-News/2012/Newark-mayor-seeks-probe-of-NYPD-Muslim-spying.

LICENSE PLATE READERS ARE WIDELY USED BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES

License plate readers are already a common tool in the arsenals of many local police departments. In a 2011 survey, almost three-quarters of police agencies included in the survey reported using license plate readers — and a full 85 percent of agencies planned on increasing their use of license plate readers over the next five years.[36] Even more strikingly, the same report found that although police departments today typically only have license plate readers installed on a few vehicles, in five years these departments anticipate that, on average, plate readers will be installed on 25 percent of all patrol cars.[37] One major license plate reader manufacturer, ELSAG, states that its machines are operating in close to 1,200 agencies in all 50 states[38] and more than 5,000 agencies worldwide.[39] Another manufacturer, PIPS Technology, claims that it has deployed 20,000 machines to agencies worldwide.[40]

Not only are license plate readers widely deployed, but few police departments place any substantial restrictions on how automatic license plate readers can be used. The approach of the Pittsburg Police Department in California is typical: It states that license plate readers can be used for "any routine patrol operation or criminal investigation."[41] It makes clear that "[r]easonable suspicion or probable cause is not required."[42] While many police departments do prohibit police officers from using license plate readers for

36 Police Executive Research Forum, *How Are Innovations in Technologies Transforming Policing?*, p. 31 (Jan. 2012), http://policeforum.org/library/critical-issues-in-policing-series/Technology_web2.pdf.
37 *Id.* at p. iii.
38 Press Release, ELSAG North America, IACP 2011: ELSAG Unveils the Latest License Plate Recognition Tech. (Oct. 21, 2011), http://www.policeone.com/police-products/traffic-enforcement/license-plate-readers/press-releases/4538797-IACP-2011-ELSAG-Unveils-the-Latest-License-Plate-Recognition-Technology/; ELSAG North America, MPH-900 Deployments, http://www.elsag.com/deployment.htm.
39 ELSAG North America, References, http://www.elsag.com/references.htm.
40 Press Release, PIPS Technology, PIPS Technology, Inc. Announces Handheld OCR (Oct. 21, 2011), http://www.federalsignal.com/pdf/pressrelease/2011_10-21_PIPS_Handheld_final.pdf.
41 Pittsburg Police Department, Policy on Automated License Plate Readers (Mar. 22, 2012), Public Records Responses, p. 94, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_pittsburgpd_pittsburgca.pdf.
42 *Id.* The Milpitas, California Police Department states that the use of the department's ALPR technology is for "law enforcement investigations only." Letter from Milpitas Police Department to ACLU of Northern California (Aug. 8, 2012), Public Records Responses, p. 128, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_milpitaspd_milpitasca.pdf. Rockville, Maryland's license plate reader policy states the technology may be used for "Homeland Security applications, electronic surveillance, suspect interdiction, stolen property recovery and a number of other policing objectives." Rockville Police Department, General Order on License Plate Reader Systems (Apr. 30, 2012), Public Records Responses, p. 363, https://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_MPIA_md.pdf. The Maryland Coordination and Analysis Center, which runs a state-based regional license plate sharing center, allows participating agencies to access plate data whenever it is "related to a criminal investigation or relevant to the safety of officers and citizens." Maryland Coordination and Analysis Center, License Plate Recognition Intelligence Bulletin (Jan. 31, 2011), Public Records Responses, p.432, http://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_dnr_md%20(1).pdf.

(T)he use of license plate readers "is only limited by the officer's imagination."

— Scarsdale, NY Police Department

their own personal uses (tracking friends and loved ones, for example), these are the only restrictions. As the Scarsdale Police Department in New York puts it, the use of license plate readers "is only limited by the officer's imagination."[43]

License plate readers collect vast quantities of data on innocent people

While it is legitimate to use license plate readers to identify those who are alleged to have committed crimes, the overwhelming majority of people whose movements are monitored and recorded by these machines are innocent, and there is no reason for the police to be keeping records on their movements. Ordinary people going about their daily lives have every right to expect that their movements will not be logged into massive government databases.

The vast majority of license plate data are collected from people who have done nothing wrong at all. Often, only a fraction of 1 percent of reads are hits — and an even smaller fraction result in an arrest.

In our records requests, documents from Maryland illustrate this point. Approximately three-quarters of Maryland's law enforcement agencies are networked into Maryland's state data fusion center, which collected more than 85 million license plate records in 2012 alone.[44] According to statistics compiled by the fusion center for that year to date through May:[45]

- Maryland's system of license plate readers had over 29 million reads. Only 0.2 percent of those license plates, or about 1 in 500, were hits. That is, only 0.2 percent of reads were associated with any crime, wrongdoing, minor registration problem, or even suspicion of a problem.
- Of the 0.2 percent that were hits, 97 percent were for a suspended or revoked registration or a violation of Maryland's Vehicle Emissions Inspection Program.

---

43 Scarsdale Police Department, General Order on ELSAG Automatic License Plate Readers (Sept. 1, 2008), Public Records Responses, p. 12638, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_scarsdalepolicedepartment_scarsdaleny_1.pdf.

44 Governor's Office of Homeland Security, *Intelligence/Information Sharing* (Dec. 2012), http://www.gohs.maryland.gov/ii_sharing_accomplishments.html.

45 Maryland Coordination and Analysis Center, Networked Mobile License Plate Reader Alerts (May 2012), Public Records Responses, p. 440, http://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_msp_md%20(1).pdf.

> While these vehicles perhaps should not be on the road, they are not the dangers to society that law enforcement agencies routinely describe when justifying their use of license plate readers.

For every one million plates read in Maryland, only 47 were potentially associated with more serious crimes—a stolen vehicle or license plate, a wanted person, a violent gang or terrorist organization, a sex offender, or Maryland's warrant-flagging program. Furthermore, even these 47 alerts may not have helped the police catch criminals or

prevent crimes. While people on the violent gang, terrorist, and sex offender lists are under general suspicion, they are not necessarily wanted for any present wrongdoing.[46]

In short, Maryland's license plate readers collect massive amounts of data, almost none of which are tied to any known or even suspected wrongdoing. Even the vast majority of hits are for minor regulatory violations.

While Maryland provided us with the clearest data on this practice, we found similar patterns across the country:

TOWN/CITY	COLLECTION PERIOD	PLATE READS STORED	HIT RATE
Burbank, IL [i]	August 2011– July 2012	706,918	0.3%
Rhinebeck, NY [ii]	January– March 2012	99,771	0.01%
High Point, NC [iii]	August 2011– June 2012	70,289	0.08%

i. Burbank Police Department, Reads Statistics (July 31, 2012), Public Records Responses, pp. 10886-902, http://www.aclu.org/files/FilesPDFs/ALPR/illinois/alprpra_burbankpd_burbankil.PDF.
ii. Rhinebeck Police Department, Quarterly License Plate Reader Progress Reports (2011 & 2012), Public Records Responses, p.12621-22, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_rhinebeckpolicedepartment_rhinebeckny_1.pdf. Seven suspended licenses, thirteen suspended registrations, five uninsured motor vehicles, and one unlicensed operator. Id.
iii. High Point Police Department, Reads Statistics (Aug. 12, 2012), Public Records Responses, pp. 801-10, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_HighPointPD_HighPointNC%20(3).pdf.

The above information reflects the hit rate, which is the best evidence of efficacy most agencies provided but is imperfect because hits are not always accurate or even generated based upon the suspicion that someone is violating the law. A more helpful statistic is provided by the Minnesota State Patrol. Of the 1,691,031 plates scanned between 2009-2011, just 852 citations were issued and 131 arrests were made.[47] That is 0.05 percent of plate reads.

Again, there is no problem with the use of license plate readers to identify individuals suspected of violating the law. But the above data provide a striking illustration of the wide dragnet that license plate readers often cast. Because they snap pictures of every passing vehicle, they generate millions of data points on the movements of individuals whom no one suspects of violating any law.

46 According to government training materials, placement on its "violent gang or terrorist" list is "based on investigative information not previously subject to independent judicial review," and indicates that someone is of interest, not that they are wanted for a crime. Violent Gang and Terrorist Organization File, *Operator's Lesson Plan* (Feb. 2005), http://www.in.gov/isp/files/Violent_Gang_Terrorist_Organization_File.pdf

47 Minnesota State Patrol, License Plate Reader Data Totals, Public Records Responses, p. 753, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(6).pdf.

Many agencies retain data on innocent Americans for long periods of time

There is no reason for law enforcement agencies to retain data on the comings and goings of innocent Americans. While holding onto "hit" data while an investigation or case is ongoing is legitimate, law enforcement agencies should not be storing data about people who have done nothing wrong.

Some law enforcement agencies delete non-hit data rapidly, proving that such privacy-protective practices are workable:

- The Ohio State Highway Patrol's license plate reader policy states that "all 'non-hit' [license plate reader] captures shall be deleted immediately." It further specifies that license plate reader "captures shall not be collected, stored, or shared with the intent of data mining."[48]
- The Minnesota State Patrol keeps license plate data for 48 hours before deleting it, keeping data longer only when there are "extenuating circumstances."[49]

Some other police departments, while not as quick to delete as the departments above, also keep data for relatively short periods of time:

- Brookline, Mass., retains data for 14 days.[50]
- Police in Tiburon, Calif., delete all license plate reader data after 30 days or less.[51]

Deleting data quickly prevents license plate reader systems from compiling huge storehouses of our location information. The Minnesota State Patrol, for example, scans tens of thousands of license plates per month — a total of almost 1.7 million plates over three years.[52] However, in the absence of "extenuating circumstances," the agency has

---

48 Ohio State Highway Patrol, Policy on Mobile and Stationary License Plate Recognition (Dec. 23, 2008), Public Records Responses, p. 14851, http://www.aclu.org/files/FilesPDFs/ALPR/ohio/14749-14851%20Department%20of%20Public%20Safety.pdf.

49 Minnesota State Patrol, General Order on License Plate Readers (Sept. 28, 2009), Public Records Responses, p. 730, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(3).pdf; Email from Minnesota State Patrol to ACLU of Minnesota (Aug. 9, 2012), Public Records Responses, p. 733, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(4).pdf.

50 Shawn Musgrave, License Plate-Reading Devices Fuel Privacy Debate, Boston Globe (Apr. 9, 2013), http://www.bostonglobe.com/metro/2013/04/08/big-brother-better-police-work-new-technology-automatically-runs-license-plates-everyone/1qoAoFfgp31UnXZT2CsFSK/story.html

51 Tiburon Town Council Minutes (Mar. 4, 2009), Public Records Responses, p. 7201, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_tiburonpd_tiburonca%20(1).pdf; Tiburon Town Council Minutes (Nov. 18, 2009), Public Records Responses, pp. 7234-35, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_tiburonpd_tiburonca%20(1).pdf.

52 Minnesota State Patrol, License Plate Reader Data Totals, Public Records Responses, pp. 750-53, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(7).pdf.

Retention policies: All over the map

a policy of deleting all license plate data 48 hours after it is collected.[53] As a result, the amount of data in the agency's possession, according to a document we obtained, "depends on the day."[54] Given that records show the daily number of plate scans rarely

53 Minnesota State Patrol, General Order on License Plate Readers (Sept. 28, 2009), Public Records Responses, p. 730, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(3).pdf.

54 Email from Minnesota State Patrol to ACLU of Minnesota (Aug. 9, 2012), Public Records Responses, p. 733, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(4).pdf.

exceeds 10,000, it is unlikely that the number of records would be more than 20,000 in a 48-hour period.[55]

In the absence of tight retention time limits, police departments rapidly accumulate vast stores of location tracking data — again, nearly all of it on innocent people. For example:

- The Piedmont Police Department in California produced records showing that it had accumulated 1,641,841 scanned records in the time period between August 2011 and August 2012. These records were still in storage as of Aug. 8, 2012.[56]
- In September 2012, Grapevine, Texas (a city in the Dallas-Fort Worth metropolitan area) reported scanning on average 14,547 plates a day and had nearly 2 million plates in its database.[57]
- Jersey City, N.J., collected 2.1 million plate reads in 2012.[58] Because a New Jersey attorney general directive compels all law enforcement agencies in the state to ensure that license plate reader data is retained for five years, assuming that 2012 is representative, it is likely that there are approximately 10 million plate reads stored at any given time.[59]

See page 20 for a selection of the retention policies we have obtained, demonstrating the range of existing data retention periods around the country.

All the pieces are lining up for widespread sharing of license plate reader data

The mass collection and retention of plate data about innocent Americans is alarming in and of itself, but it is all the more worrying because these data are increasingly being fed into larger regional databases. These databases can be in the possession and control of other government jurisdictions. Once a law enforcement agency shares data, it can lose any say about how these data are used, stored, and shared.

---

55 Minnesota State Patrol, License Plate Reader Data Totals, Public Records Responses, pp. 750-53, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(7).pdf.

56 PRA Response letter from Piedmont PD (Aug. 9, 2012), Public Records Responses, pp. 22341-43, http://www.aclu.org/files/FilesPDFs/ALPR/california/22341-22396 Piedmont PD ALPR Response (1901-56).pdf.

57 Letter from Grapevine Police Department to ACLU of Texas (Sept. 10, 2012), Public Records Responses, p. 2424, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_grapevinePD_grapevineTX(6).pdf.

58 Jersey City, Reads Statistics, Public Records Responses, p. 17584, https://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/17569-17584 Jersey City Supp OPRA Response 2 of 8.pdf.

59 New Jersey Attorney General, Guidelines for the Use of Automated License Plate Readers and Data (Dec. 3, 2010), Public Records Responses, p. 6144, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/alprpra_divisionofcriminaljustice_trentonnj_1%20(6).pdf.

That said, today many law enforcement agencies share license plate reader data on a case-by-case basis in response to specific requests from other law enforcement agencies (and a few report no sharing).[60] Requiring a case-by-case demonstration of need is preferable to wholesale sharing because it ensures that data about innocent people isn't needlessly spread to additional government computer systems, a step that increases the risk of its being misused or wrongfully disclosed.

However, there are already examples of license plate reader data being systematically pooled into large regional databases:

- **Greenbelt, Md.,** feeds plate information into the state fusion center, the Maryland Coordination and Analysis Center (MCAC),[61] and also participates in a regional database called the National Capital Region LPR Project (NCR),[62] which collects plate information from police departments in Washington, D.C., Virginia, and Maryland.[63] Although Greenbelt's policy is to purge data from its local hard drive after 30 days,[64] its sharing practices undercut that policy. MCAC stores all license plate data for one year, no matter what the

Text continues on p. 22.

60 For example, Grapevine, Texas, Jacksonville, North Carolina, and Mesquite, Texas do not allow third parties to access their license plate data, while Hutchinson, Kansas and the Minnesota State Patrol only share data when a specific request is made. The City of El Paso, Texas shares license plate reader data for "legitimate law enforcement purposes." Newark, Delaware complies with requests from other law enforcement agencies for specific license plate reads "related to criminal or traffic investigations." Lincoln, Nebraska shares license plate reader data only in response to an inquiry made by a prosecutor or defense attorney in an active criminal case. Letter from Grapevine Police Department to ACLU of Texas (Sept. 10, 2012), Public Records Responses, p. 2424, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_grapevinePD_grapevineTX(6).pdf; Letter from Jacksonville Police Department to ACLU of North Carolina (Aug. 21, 2012), Public Records Responses, p. 1481, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_jacksonvillepd_jacksonvillenc.pdf; Mesquite Police Department, Response to ACLU of Texas Records Request, Public Records Responses, p. 10466, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_mesquitepd_mesquitetx%20(2).pdf; Email from Hutchinson Police Department to ACLU of Kansas and Western Missouri (Aug. 3, 2012), Public Records Responses, p. 342, http://www.aclu.org/files/FilesPDFs/ALPR/kansas/alprpra_hutchinsonpd_hutchinsonka.pdf; Email from Minnesota State Patrol to ACLU of Minnesota (Aug. 9, 2012), Public Records Responses, p. 733, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_stpaulmn_1%20(4).pdf; City of El Paso, License Plate Reader Policy and Guidelines, Public Records Responses, p. 10078, http://www.aclu.org/files/FilesPDFs/ALPR//texas/alprpra_elpasoPD_elpasotx%20(5).pdf; Letter from Newark City Solicitor to ACLU of Delaware (Oct. 1, 2012), Public Records Responses, p. 7559, https://www.aclu.org/files/FilesPDFs/ALPR/delaware/7558-7559 City of Newark FOIA Response.pdf; Letter from Lincoln Police Department to ACLU of Nebraska (Sept. 7, 2012), Public Records Responses, p. 4683, http://www.aclu.org/files/FilesPDFs/ALPR/nebraska/alprpra_lincolnpolicedepartment_lincolnne_1.pdf.

61 Letter from Maryland Governor's Office of Crime Control & Prevention to Greenbelt Police Department (Mar. 21, 2011), Public Records Responses, p. 27406, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-7-greenbelt-police; Maryland's LPR Program and Policy Overview: How We Differ from Most Agencies and Why (2011), http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Maryland%27s-LPR-Program-and-Policy-Overview.pdf. Approximately three quarters of Maryland's law enforcement agencies are networked into MCAC, and the fusion center collected more than 85 million license plate records in 2012 alone. Governor's Office of Homeland Security, Intelligence/Information Sharing (Dec. 2012), http://www.gohs.maryland.gov/ii_sharing_accomplishments.html.

62 Addendum to 2008 Grant Agreement for ALPR Equipment between Arlington County, Virginia and City of Greenbelt, Maryland (Mar. 28, 2012), Public Records Responses, pp. 27378-81, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-6-greenbelt-police; Memorandum of Understanding between National Capital Region's License Plate Reader Information Sharing Program and Greenbelt Police (Mar. 28, 2012), Public Records Responses, pp. 27384-90, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-6-greenbelt-police.

63 Prince William County Government, Motion to Approve MOU for the National Capital Region's License Plate Reader Information Sharing Program (July 17, 2012), http://eservice.pwcgov.org/documents/bocs/agendas/2012/0717/4-h.pdf.

64 City of Greenbelt, Response to ACLU of Maryland Records Request (Sept. 5, 2012), Public Records Responses, pp. 27367-68, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-6-greenbelt-police.

Automatic license plate reader retention periods around the country

JURISDICTION	PLATE DATA RETENTION PERIOD			
	1 to 30 days	31 days to 1 yr	1 to 5 years	Indefinite
Minnesota State Patrol	48 hours			
Burbank, IL	21 days			
Deerpark, NY	30 days			
Jacksonville, NC	30 days			
Schenectady, NY		35 days		
New Paltz, NY		50 days		
Boston, MA		90 days		
Fishkill, NY		90 days		
Franklin County, OH		90 days		
Sugar Land, TX		90 days		
Raleigh, NC		6 months		
New Castle County, DE		360 days		
Dutchess County, NY		1 year		
High Point, NC		1 year		
Highland Village, TX		1 year		
Charlotte-Mecklenburg, NC			18 months	
Aurora, CO			2 years	
Commerce City, CO			2 years	
Los Angeles County, CA			2 years	
Plano, TX			2 years	
Delaware Dept of Homeland Security			5 years	
New Jersey			5 years	
Grapevine, TX				Presumed indefinite
Mesquite, TX				Indefinite retention
Yonkers, NY				Indefinite retention

NOTE: Retention periods generally refer to non-hit data that has not been flagged as part of an investigation or incident. Exact policies vary but usually cover the vast majority of automatic license plate reader reads.

i. Minnesota State Patrol, General Order on License Plate Readers (Sept. 26, 2009), Public Records Responses, p. 730, http://www.aclu.org/files/FilesPDFs/ALPR/minnesota/alprpra_minnesotastatepatrol_alprpra.pdf.

ii. Burbank Police Department, General Order on Automated License Plate Recognition Systems (Nov. 1, 2011), Public Records Responses, p. 10702, http://www.aclu.org/files/FilesPDFs/ALPR/illinois/alprpra_burbankpd_burbankil.PDF.

iii. Deerpark Police Department, Special Order on License Plate Readers (Dec. 16, 2010), Public Records Responses, p. 1217, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_townofdeerparkpolicedepartment_deerparkny_1.pdf.

iv. Letter from Jacksonville Police Department to ACLU of North Carolina (Aug. 21, 2012), Public Records Responses, p. 1490, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_jacksonvillenc_jacksonvillenc.pdf.

v. Schenectady Police Department, Response to New York Civil Liberties Union Records Request (Oct. 31, 2012), Public Records Responses, p. 15589, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_schenectadypolicedepartment_schenectadyny_1.PDF.

vi. Letter from New Paltz Police Department to New York Civil Liberties Union (Aug. 8, 2012), Public Records Responses, p. 12933, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_newpaltzpolicedepartment_newpaltzny_1.pdf.

vii. Boston Police, Special Order on License Plate Recognition System (Sept. 14, 2011), Public Records Responses, p. 4793, http://www.aclu.org/files/FilesPDFs/ALPR/massachusetts/4790-4792_Boston_Special_Order_11_029.pdf.

viii. Letter from Fishkill Police Department to New York Civil Liberties Union (Sept. 17, 2012), Public Records Responses, p. 12225, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_fishskillpolicedepartment_fishskillny_1.pdf.

ix. Revised Memorandum of Understanding between Franklin County Sheriff's Office and Agency Police Department, Outside Region #4, Public Records Responses, p. 14866, http://www.aclu.org/files/FilesPDFs/ALPR/ohio/14862%20-14874%20Franklin%20County.pdf.

x. Sugar Land Police Department, General Order on Use of LPR Technology (Aug. 26, 2011), Public Records Responses, p. 14595, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_sugarlandpd_sugarlandtx%20(2).pdf.

xi. Raleigh Police Department, Directive on Automated License Plate Recognition and Internet Protocol Camera System (Sept. 5, 2012), Public Records Responses, p. 4055, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_raleighnc_raleighnc.pdf.

xii. Letter from New Castle County Attorney to ACLU of Delaware (Aug. 31, 2012), Public Records Responses, p. 2284, http://www.aclu.org/files/FilesPDFs/ALPR/delaware/alprpra_nac_newcastlecountyde%20(1).pdf.

xiii. Dutchess County Sheriff's Office, Response to New York Civil Liberties Union Records Request (Dec. 7, 2012), Public Records Responses, p. 14743, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_dutchesscountysheriffsoffice_poughkeepsieny_1.pdf.

xiv. High Point Police Department, General Order on Automated License Plate Readers (June 1, 2011), Public Records Responses, p. 811, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_HighPointPD_HighPointNC%20(3).pdf.

xv. Highland Village Police Department, General Order on Automated License Plate Readers (Sept. 23, 2011), Public Records Responses, p. 2624, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_highlandpd_highlandvillagetx%20(7).pdf.

xvi. Charlotte-Mecklenburg Police Department, Standard Operating Procedure on License Plate Readers (Apr. 29, 2011), Public Records Responses, p. 1250, http://www.aclu.org/files/FilesPDFs/ALPR/north-carolina/alprpra_charlotte_mecklenburgpd_charlotte-mecklenburgnc%20(1).pdf.

xvii. Aurora Police Department, Special Order on Automated License Plate Readers (Dec. 14, 2011), Public Records Responses, p. 7908, http://www.aclu.org/files/FilesPDFs/ALPR/colorado/alprpra_auroragpd_auroracp%20(2).pdf.

xviii. Commerce City Police, Policy and Procedures Manual (Feb. 1, 2011), Public Records Responses, p. 7916, http://www.aclu.org/files/FilesPDFs/ALPR/colorado/alprpra_commercecitypd_commercecitycp%20(3).pdf.

xix. Los Angeles County Sheriff's Department, Field Operations Directive on Automated License Plate Recognition (ALPR) System (Aug. 17, 2009), Public Records Responses, p. 4886, http://www.aclu.org/files/FilesPDFs/ALPR/missouri/alprpra_professionaldevelopmentandresearchbureau_kansascitymo_1.pdf.

xx. Email between Plano Police Department and PlateScan (May 11, 2010), Public Records Responses, p. 13704, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_planopd_planotx%20(16).pdf.

xxi. Delaware State Police, Automated License Plate Reader Policy (Sept. 2010), Public Records Responses, p. 4743, http://www.aclu.org/files/FilesPDFs/ALPR/delaware/alprpra_delawarestatepolice_de.pdf.

xxii. New Jersey Attorney General, Guidelines for the Use of Automated License Plate Readers and Data (Dec. 3, 2010), Public Records Responses, p. 6144, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/alprpra_divisionofcriminaljustice_njstatepo_13%20(2).pdf.

xxiii. Letter from Grapevine Police Department to ACLU of Texas (Sept. 10, 2012), Public Records Responses, pp. 2423-24, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_grapevinepd_grapevinetx(2).pdf.

xxiv. Mesquite Police Department, Response to ACLU of Texas Records Request, Public Records Responses, pp. 1044-54, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_mesquitepd_mesquitetx%20(2).pdf.

xxv. See generally Documents from Yonkers Department of Law in Response to New York Civil Liberties Union Records Request, Public Records Responses, pp. 15894-15940, http://www.aclu.org/files/FilesPDFs/ALPR/new-york/alprpra_yonkerspolicedepartment_yonkersny_1.pdf.

retention policies are of the police department that collected it.[65] It is unclear what NCR's retention policy is, or whether it even has one, but when license plate information is shared via NCR's system, the receiving agency may store and use that data "in compliance with [its own] data retention policy."[66] Accordingly, any law enforcement agencies obtaining Greenbelt's data through NCR may retain it indefinitely.

- License plate data are widely shared in **California's Bay Area** through the Northern California Regional Intelligence Center (NCRIC), although the full extent of sharing is not publicly known.[67] According to a May 2012 document, this fusion center's goal is to collect license plate information from approximately 22 police departments, and grant access to several more.[68] NCRIC maintains a broad mandate for its use of license plate information — in addition to law enforcement, NCRIC maintains that it may use license plate information for the "protection of special events; protection of critical infrastructure; and responding and mapping the license plate landscape of critical events."[69]
- Very little was known about the use of automatic license plate readers in **Vermont** before the ACLU of Vermont joined with other ACLU affiliates across the country in public records requests for information. The ACLU of Vermont learned that police departments in all parts of the state were using them, data was being uploaded to a centralized computer database and retained for four years, and no statutes or rules were in place to govern their use. A new law sets statewide regulations.[70] The law shortens to 18 months the length of time data may be retained (with longer preservation of data allowed with a court order), clearly defines who can have access to the data and under what circumstances, and requires annual reporting on the use of automatic license plate readers and data requests.

---

65 Maryland Coordination and Analysis Center, Automatic License Plate Recognition Program Standard Operating Procedure, p. 3 (2012), http://www.mcac.maryland.gov/resources/LPR/20120809_MCAC_LPR_SOP.pdf; City of Greenbelt, Presentation on ELSAG Automated License Plate Reader & Mobile Plate Hunter 900, Public Records Responses, p. 27451, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-3-greenbelt-police.

66 National Capital Region's License Plate Reader Information Sharing Program, Program Requirements, Public Records Responses, p. 27380, https://www.aclu.org/national-security-technology-and-liberty/response-public-records-request-6-greenbelt-police.

67 County of San Mateo, NCRIC Answers to Questions Submitted from Potential Vendors, p. 2 (May 22, 2012), http://www.co.sanmateo.ca.us/Attachments/sharedservices/PDFs/RFP/2012/NCRIC%20RFP1266%20Answers%20To%20Vendor%20Qs.pdf.

68 *Id.*

69 *Id.* at pp. 22737-40.

70 23 V.S.A. § 1607, http://www.leg.state.vt.us/docs/2014/Acts/ACT069.pdf.

PUSHING BACK ON INVASIVE LICENSE PLATE READER USE

A Success Story

With a little bit of organizing effort and access to the right information, local communities can act to ensure that police departments implement sensible, privacy-protective license plate reader policies.

That's what happened in Brookline, Mass., where the ACLU of Massachusetts and local activists came together to work with the city government to implement a data policy that both enables law enforcement to use the tool to great public safety benefit and mitigates the serious privacy harms that result from its unregulated deployment.

Kade Crockford, director of the Technology for Liberty Project at the ACLU of Massachusetts, tells the story:

Massachusetts has a fairly unique town government structure, but people who live in states with strong town or county powers can follow the Brookline model to great effect. Our organizing followed some basic principles.

First, find out what's going on. In order to do that, we did a cursory web search to see what kind of information existed in the public sphere. We found that the state had recently received funding from the federal government that it planned to use to purchase license plate readers for city and state law enforcement. Alarmingly, the state website describing the grant said that all police departments that received funds would be required to submit all captured license plate data to the state criminal justice database. That alerted us to a serious threat: the possibility that the state would amass detailed records of our driving habits, all without warrants or any probable cause whatsoever.

Next we filed a public records request to find out which cities and towns had received funding from the state. Upon receiving those records, we learned that Brookline — an affluent Boston suburb with a higher-than-average ratio of privacy advocates to residents — was on the list.

We then began the next phase of our organizing: getting the word out.

Working with activists in Brookline, we penned op-eds in the local newspapers, warning residents and town government officials that if the police accepted the state

grant money, all of their motoring movements would be shared with the state, and the city would lose control over the data forever. It made for a convincing argument, and the local government held a hearing about the matter.

The last step was turning out like-minded people to join us in raising concerns. We asked interested residents to come to the hearing to deliver testimony arguing that the local government should reject the license plate reader grant.

After much back and forth with the town government and lots of discussion in the local media, Brookline's Board of Selectmen eventually agreed with us and the town's privacy advocates: The plan's risks outweighed its benefits. The grant was voted down. Ultimately, our arguments had been so winning that even the chief of police — a major advocate of license plate reader technology — agreed that it was probably best to skip the state's grant, since it was tied to data sharing requirements that put Brookline residents at risk for privacy violations.

But the fight still wasn't over.

The police really wanted a license plate reader, and were willing to purchase it without the help of the state grant. So we continued to work with the police department, the town government, and local activists, submitting comments on a proposed license plate reader policy that required the police to delete data after 14 days unless it was evidence of a crime or infraction, or the police were required to retain it by law. The ACLU doesn't agree with everything in the Brookline policy, but it nonetheless stands out as one of the best we've seen nationwide, with a data retention period of 14 days.

After we successfully raised the issue throughout the town, the government knew that it had to consider the public's input before approving any license plate reader or policy. We found that the democratic process worked, as long as ordinary people were willing to put the work in. Our organizing effort showed that active, alert residents can affect major policy decisions on the local level.

If you have the time and energy to invest in holding your police department accountable, you can do it, too. If you aren't sure about whether or not your department uses license plate readers or has a good data policy, go to your next local government meeting and raise the issue.

A little effort goes a long way towards making sure we are both safe and free, no matter what technologies come down the road.

THE FEDERAL GOVERNMENT IS FUELING STATE AND LOCAL USE OF LICENSE PLATE READERS

Federal funding has fueled the spread of license plate readers among state and local law enforcement agencies. The Wall Street Journal reported in 2012 that, over the past five years, the Department of Homeland Security distributed over $50 million in grants to fund the acquisition of license plate readers.[71] Company materials corroborate the major role that federal funding plays. According to a government "grant guide" on the website of license plate reader manufacturer ELSAG North America, the Department of Homeland Security has distributed "billions of dollars in grants" through the Homeland Security Grant Program and the Infrastructure Protection Program.[72] ELSAG's website also states that the Justice Department is the "lead Federal funding agency."[73] Federal money plays such a critical role in supporting the purchase of license plate readers that PIPS Technology, another major manufacturer, maintains Grant Assistance Coordinators on staff to work directly with police departments applying for government funds.[74]

Documents obtained by the ACLU are replete with examples of local and state agencies building license plate reader networks with federal grant money. Police departments that would otherwise be limited by local budgets have received tens of thousands or hundreds of thousands of dollars from the federal government to establish or expand license plate reader programs. To provide just a few examples:

- Many police departments received grants from the Department of Homeland Security. For example, San Rafael, Calif., purchased four license plate reader cameras with a grant of $19,040.[75] El Paso County, Texas, purchased license plate readers with $90,000 out of a $2.5 million grant to improve security at the U.S. border.[76]
- The Department of Justice was also a key source of funding. For example, New Castle County, Del., purchased a system that included eight license plate readers

71 Angwin & Valentino-Devries, *supra* note 10.
72 ELSAG North America, Grant Guide, http://elsag.com/grant_guide.htm.
73 *Id.*
74 PIPS Technology, Police Grants Help, http://pipstechnology.com/contact/grants/.
75 San Rafael City Council, Resolution No. 13309 (Mar. 19, 2012), Public Records Responses, pp. 3-4, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_sanrafaelpd_sanrafaelca%20(1).pdf.
76 CBP, Revised Operations Order Report FY 2011, Operation Stonegarden El Paso (July 16, 2012), Public Records Responses, p. 2371, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_elpasosheriffsoffice_elpasotx%20(3).pdf.

with a grant of $200,000.[77] Hutchinson, Kan., purchased a system that included four license plate readers with a grant of $24,000.[78] The Maryland Transportation Authority Police purchased a system that included 14 license plate readers with a grant of $161,000.[79] Edison, N.J., purchased one license plate reader with $20,223 out of a $22,076 grant.[80] Cheyenne, Wyo., purchased a system that included two license plate readers with $19,017.63 out of a $48,472 grant.[81]

---

77 DOJ Memo to New Castle County Police Department and Invoices (Aug. 21, 2009), Public Records Responses, p. 9287-93, http://www.aclu.org/files/FilesPDFs/ALPR/delaware/alprpra_ncc_newcastlecountyde (2).pdf.

78 Letter from Kansas Criminal Justice Coordinating Council to Hutchinson Police Department (June 8, 2011), Public Records Responses, p. 351, https://www.aclu.org/files/FilesPDFs/ALPR/kansas/alprpra_hutchinsonpd_hutchinsonka (4).pdf; Invoices from PIPS Technology (Apr. 28, 2011), Public Records Responses, p. 349, https://www.aclu.org/files/FilesPDFs/ALPR/kansas/alprpra_hutchinsonpd_hutchinsonka (3).pdf.

79 Letter to Maryland Transportation Authority Police (July 31, 2009), Public Records Responses, p. 534, http://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_MarylandTransportationAuthorityandPolicy_md.pdf; Maryland Transportation Authority Special Report (Aug. 11, 2009), Public Records Responses, p. 535, http://www.aclu.org/files/FilesPDFs/ALPR/maryland/alprpra_MarylandTransportationAuthorityandPolicy_md.pdf.

80 Letter from Edison Police Department to New Brunswick Police Department (Apr. 17, 2012), Public Records Responses, p. 16804, http://www.aclu.org/files/FilesPDFs/ALPR/new-jersey/16802-16810 Edison 2nd Supp Response.pdf.

81 DOJ Grant Award Letter and Invoice (Aug. 19, 2011), pp. 3976-78, http://www.aclu.org/files/FilesPDFs/ALPR/wyoming/alprpra_cheyennepolicedepartment_cheyennewy_1.pdf.

TOO LITTLE IS KNOWN ABOUT THE FEDERAL GOVERNMENT'S OWN USE OF LICENSE PLATE READERS

In addition to funding state and local purchases of license plate readers, some federal agencies maintain their own networks of license plate readers across the United States, and engage in data-sharing on a national level. Unfortunately, too little is known about how the federal government uses license plate data. As part of our public records initiative we filed Freedom of Information Act requests with the Departments of Justice, Homeland Security, and Transportation, but received few voluntary responses and have had to file a federal lawsuit to force the departments to respond. As of this writing, that litigation is ongoing (we will update this report once we obtain responsive documents).

For now, here is what we do know:

- Customs and Border Protection uses license plate readers to scan the license plates of almost every car entering the United States, as well as many cars leaving the country.[82]
- Immigration and Customs Enforcement has experimented with operating license plate readers as well.[83] It has also looked into purchasing access to private repositories of plate data.[84]
- The Drug Enforcement Administration had deployed cameras in Arizona, Texas, New Mexico, and California as of 2012,[85] and was working to expand its network of license plate readers throughout the northern and southern borders, as well as in "hub cities and the high-traffic corridors."[86]

---

82 DHS reports indicate that since 2009, CBP's license plate readers have logged "nearly 100 percent of land border traffic." Department of Homeland Security, Northern Border Strategy, p. 17 (June 2012), http://www.dhs.gov/xlibrary/assets/policy/dhs-northern-border-strategy.pdf.

83 ICE National Bulk Cash Smuggling Center, internal email (Sept. 13, 2011), Public Records Responses, p. 16167, http://www.aclu.org/files/FilesPDFs/ALPR/federal/ICE/16147-16228%20r_Pages%20from%20Bulk%20Cash%20Combined-1.pdf.

84 ICE, internal emails (Jan. 2011), Public Records Responses, pp. 21223-24, https://www.aclu.org/files/FilesPDFs/ALPR/federal/ICE/21201-21224 r_ALPR Privacy Documents.pdf.

85 G.W. Schultz, *DEA installs license-plate recognition devices near Southwest border*, Ars Technica (July 11, 2012), http://arstechnica.com/tech-policy/2012/07/dea-installs-license-plate-recognition-devices-near-southwest-border/.

86 Jay Stanley, *DEA Recording Americans' Movements on Highways, Creating Central Repository of Plate Data*, ACLU Free Future (May 18, 2012), http://www.aclu.org/blog/technology-and-liberty-criminal-law-reform/dea-recording-americans-movements-highways-creating.

PRIVATE COMPANIES COLLECT LICENSE PLATE DATA WITH NO OVERSIGHT

License plate readers are used not only by law enforcement agencies but also by private companies. This has led to the emergence of numerous privately owned databases containing the location information of vast numbers of Americans.

License plate readers are used in a variety of non-law enforcement roles. Private companies use license plate readers to monitor airports, control access to gated communities, enforce payment in parking garages, and even help customers find their cars in shopping mall parking lots.[87] While these uses in and of themselves are not objectionable, private companies can scan thousands of plates each day and store information indefinitely, creating huge databases of Americans' movements.

Perhaps the largest private users of license plate readers are repossession agents who have recognized the value of license plate location information and built enormous private databases with data from all over the country. MVTrac, one of the biggest companies in this industry, claims to have photographs and location data on "a large majority" of registered vehicles in the United States,[88] while the Digital Recognition Network (DRN) boasts of "a national network of more than 550 affiliates."[89] These affiliates, most of whom are repossession agents, are located in every major metropolitan area of the United States. DRN fuels rapid growth of its database by offering to fully finance up to five automatic license plate readers for affiliates located in major metropolitan areas, such as New York, Los Angeles, Orlando, Boston, and Washington, D.C., which guarantee they will provide DRN with a minimum of 50,000 aggregate plate scans per month.[90] DRN affiliates feed location data on up to 50 million vehicles each month (nearly all of which are not wanted for repossession) into DRN's national database.[91] This database now contains over 700 million data points on where American drivers have been.[92]

Private companies have partnerships with law enforcement. Police departments

---

87 Michael Harlow, *License Plate Recognition: It's Grown Far Beyond Airports*, Parking Today (July 2009), http://www.parkingtoday.com/articledetails.php?id=788; Martha Groves, *Servant or Snoop in the Parking Garage?*, L.A. Times (Jan. 23, 2011), http://articles.latimes.com/2011/jan/23/local/la-me-santa-monica-parking-20110123.

88 Angwin & Valentino-Devries, *supra* note 10.

89 Digital Recognition Network, http://www.drndata.com/index.html.

90 MVConnect, LLC et al v. Recovery Database Network, Inc. et al, No. 3:10-cv-01948 (N.D. Tex. Jan. 20, 2011), Amended Complaint, Exhibit 8, ECF No. 31-8. Title to the ALPRs is not transferred from DRN to the affiliates until they have contributed a total of 1,000,000 plate scans.

91 Digital Recognition Network, http://www.drndata.com/index.html.

92 *Id.*

can purchase license plate reader data from private corporations. For example, law enforcement agencies can access MVTrac's database and search through data collected by private repossession agencies.[93] DRN contributes its affiliate-generated data to the National Vehicle Location Service (NVLS), which is run by Vigilant Solutions, a partner of DRN. NVLS aggregates DRN's data with data received from other private sources, such as access control and parking systems, and from law enforcement agencies.[94] According to Vigilant, NVLS "is the largest [license plate] data sharing initiative in the United States."[95] The database holds over 800 million license plate reader records,[96] and is used by over 2,200 law enforcement agencies and 25,000 United States law enforcement investigators.[97] Each month, the system adds roughly 1,000 new users[98] and grows by 35 to 50 million license plate reader records.[99] Law enforcement agencies that use or have used NVLS include the Milpitas Police Department in California,[100] police in Port Arthur, Texas,[101] and Immigration and Customs Enforcement.[102]

These private databases raise serious privacy concerns. Their massive size suggests that they contain a great deal of information about our movements. These huge databases of plate information are not subject to any data security or privacy regulations governing license plate reader data. These companies decide who can access license plate data and for what purposes.

Last year, California considered a bill[103] that would have required private companies to delete license plate records after 60 days and regulated the sale and sharing of privately held plate data. Due in part to the companies' vigorous opposition, as well as that of law enforcement agencies, the bill died on the Senate floor.[104] Today, these companies continue to operate with no regulation of how they use the data they are rapidly collecting.

---

93 Angwin & Valentino-Devries, *supra* note 10; MVTRAC, Law Enforcement, http://mvtrac.com/law-enforcement/; MVTRAC, MVENFORCE, http://mvtrac.com/law-enforcement/mvenforce/.

94 Vigilant Solutions, National Vehicle Location Service FAQs, http://nvls-lpr.com/nvls/nvls_faq.html?pp=1#ans9.

95 Vigilant Solutions, National Vehicle Location Service (NVLS), http://vigilantsolutions.com/products/nvls.

96 Vigilant Video, National Vehicle Location Service, p. 2 (2012), http://vigilantsolutions.com/wp-content/uploads/2012/09/Vigilant-NVLS-Datasheet-092012.pdf.

97 *Id.*

98 *Supra* note 24.

99 Vigilant Solutions, National Vehicle Location Service (NVLS), http://vigilantsolutions.com/products/nvls.

100 Letter from Milpitas Police Department to ACLU of Northern California (Aug. 8, 2012), Public Records Responses, p. 128, http://www.aclu.org/files/FilesPDFs/ALPR/california/alprpra_milpitaspd_milpitasca.pdf.

101 Port Arthur Police Department, Invoice from Vigilant Video for Annual Subscription Renewal, Public Records Responses, p. 2062, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_portharthurPD_portarthurtx (6).pdf.

102 ICE, internal emails (Jan. 2011), Public Records Responses, pp. 21223-24, https://www.aclu.org/files/FilesPDFs/ALPR/federal/ICE/21201-21224 r_ALPR Privacy Documents.pdf.

103 S.B. 1330 (introduced on Feb. 23, 2012), http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1301-1350/sb_1330_bill_20120529_amended_sen_v96.pdf. For further discussion, *see* Farivar, *supra* note 24.

104 Press Release, Digital Recognition Network, Digital Recognition Network Defeats California SB1330 (June 5, 2012), http://web.archive.org/web/20121209024203/http://drndata.com/pdf/CASB1330Releasev2.060512.pdf; Angwin & Valentino-Devries, *supra* note 10.

DATA MINING LICENSE PLATE RECORDS

If privacy protections aren't instituted, we can expect license plate readers to be used in many new ways and new places. In particular, we can expect all kinds of cross-referencing and data mining techniques to be applied to the information streams generated by license plate reader scanners.

We could easily see scenarios such as:

- A DEA risk-analysis system alerts the police in Utah that the same car is traveling between Salt Lake City and Nogales, Ariz., on a monthly basis. The next night, a divorced father visiting his child in Arizona receives a knock on the door from federal agents to interrogate him about his travel. Drug dealer or dedicated dad? Data-mining systems can't tell the difference.
- An affluent suburbanite has a friend who lives in a poor neighborhood where drugs are often sold. The police get an alert that he is a regular visitor to this neighborhood, and he gets pulled over on a pretext ("driving erratically") several times so they can search his car, and a police "intelligence squad" opens a file on him.
- A student working nights as a bartender gets stopped frequently on suspicion of DUI because the police know that she is driving home from a bar.
- The FBI begins investigating a man because he visited a series of places — a mosque, a hardware store, and a money-transfer service — that the government's computers have flagged as "suspicious." But he's a perfectly law-abiding Home Depot employee and practicing Muslim who helps out his extended family in Somalia.
- The FBI opens a probe into the background of a kindergarten teacher because her car was parked at an apartment building — and then coincidentally again later at a store — at the same time as a man who is on a terrorist watch list. Agents appear at her workplace to interview her co-workers.

THERE ARE TOO FEW RULES IN PLACE TO PROTECT PRIVACY

Given that license plate readers facilitate the mass collection of information on Americans' movements, that too many jurisdictions are retaining data on innocent Americans for long periods of time, and the inevitable trend towards greater sharing of this data, it is apparent that there are too few rules in place to ensure that license plate reader technology is not abused.

In a small 2009 survey, over half of responding agencies that used license plate readers had no policy addressing license plate reader use.[105] Among the agencies that did have or were developing license plate reader policies, most policies did not address data retention (52 percent) or data sharing (56 percent).[106]

Only five states have laws on the books governing license plate readers, and the laws have different approaches as well as strengths and weaknesses.[107] New Hampshire all but bans license plate readers with narrow exceptions for EZ-Pass and for use by government agencies at public buildings and three named bridges in Portsmouth.[108] Maine prohibits all private use of license plate readers (except as part of an EZ-Pass system) and requires law enforcement to delete captured plate data that is not part of a criminal or intelligence investigation within 21 days.[109] Arkansas strictly limits private use of license plate readers, requires captured plate data that is not part of an ongoing investigation to be deleted within 150 days and prohibits all sharing unless it is evidence of an offense.[110]

---

105 David J. Roberts & Meghann Casanova, International Association of Chiefs of Police, *Automated License Plate Reader Systems: Policy and Operational Guidance for Law Enforcement*, p. 25 (2012), http://www.theiacp.org/portals/0/pdfs/IACP_ALPR_Policy_Operational_Guidance.pdf.

106 *Id.*

107 These states are New Hampshire, Maine, Arkansas, Vermont, and Utah. N.H. Rev. Stat. Ann. § 261:75-b (2007), http://www.gencourt.state.nh.us/rsa/html/xxi/261/261-75-b.htm; Me. Rev. Stat. tit. 29-A, § 2117-A (2010), http://www.mainelegislature.org/legis/statutes/29-a/title29-Asec2117-A.html; H.B. 1996, 89th Gen. Assemb., Reg. Sess. (Ark. 2013), http://www.arkleg.state.ar.us/assembly/2013/2013R/Acts/Act1491.pdf; Sec. 1. 23 V.S.A. § 1607, http://www.leg.state.vt.us/DOCS/2014/ACTS/ACT069.PDF; 2013 Utah Laws Ch. 447 (S.B. 196), http://le.utah.gov/~2013/bills/sbillenr/SB0196.htm. In addition, Virginia's Attorney General has issued an advisory opinion concluding that the state's Government Data Collection and Dissemination Practices Act prohibits state law enforcement's use of license plate readers for passive data collection — that is, collecting and pooling the license plate information of every car that passes them by. Instead, license plate readers can only be used "actively" — that is, in pursuit of particularly identified license plates "evaluated and determined to be relevant to criminal activity." Attorney General Opinion 12-073, p. 1 (Feb. 12, 2013), http://www.oag.state.va.us/Opinions%20and%20Legal%20Resources/OPINIONS/2013opns/12-073%20Flaherty.pdf. Also, New Jersey's Attorney General has issued a directive regarding license plate reader use. The directive requires all New Jersey law enforcement agencies to retain license plate reader data for five years and contemplates data-mining and pattern analysis of the captured plate data "to detect suspicious activities that are consistent with the modus operandi of criminals." Attorney General Directive No. 2010-05, p. 2 (Dec. 3, 2010), http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf.

108 N.H. Rev. Stat. Ann. § 261:75-b (2007), http://www.gencourt.state.nh.us/rsa/html/xxi/261/261-75-b.htm.

109 29-A M.R.S.A. § 2117-A (available on Westlaw)

110 H.B. 1996, 89th Gen. Assemb., Reg. Sess. (Ark. 2013), http://www.arkleg.state.ar.us/assembly/2013/2013R/Acts/Act1491.pdf.

RECOMMENDATIONS

To ensure that license plate readers can be used by law enforcement agents for legitimate purposes without infringing on Americans' privacy and other civil liberties, the ACLU calls for the adoption of legislation and law enforcement agency policies adhering to the following principles:

- License plate readers may be used by law enforcement agencies only to investigate hits and in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to an ongoing criminal investigation. The police must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to *generate* reasonable suspicion.
- Law enforcement agencies must not store data about innocent people for any lengthy period. Unless plate data has been flagged, retention periods should be measured in days or weeks, not months, and certainly not years.
- It is legitimate to flag plate data (1) whenever a plate generates a hit that is confirmed by an agent and is being investigated, (2) in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to a specific criminal investigation or adjudication, (3) when preservation is requested by the registered vehicle owner, or (4) when preservation is requested for criminal defense purposes.
- Once plate data has been flagged, a longer retention period commensurate with the reason for flagging is appropriate.
- Law enforcement agencies must place access controls on license plate reader databases. Only agents who have been trained in the departments' policies governing such databases should be permitted access, and departments should log access records pertaining to the databases.
- People should be able to find out if plate data of vehicles registered to them are contained in a law enforcement agency's database. They should also be able to access the data. This policy should also apply to disclosure to a third party if the registered vehicle owner consents, or for criminal defendants seeking relevant evidence.
- Law enforcement agencies should not share license plate reader data with third parties that do not conform to the above retention and access principles, and should be transparent regarding with whom license plate reader data are shared.

- Hot lists should be updated as often as practicable and, at a minimum, at the beginning of each shift. Whenever a license plate reader alerts on a plate, law enforcement, before taking any action, should be required to confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(s) match any individual(s) identified in the alert.
- Any entity that uses license plate readers should be required to report its usage publicly on at least an annual basis.

ACKNOWLEDGMENTS

This report has been a project of the American Civil Liberties Union. The primary author is Catherine Crump, staff attorney, Speech, Privacy & Technology Project. The ACLU would also like to acknowledge the following individuals who made substantial contributions to this report: Ibrahim Alsaygh, Christina Argueta, Josh Bell, David Benhamou, Tess Bloom, Allie Bohm, Stevaughn Bush, Matt Cagle, Kade Crockford, Sandra Fulton, Naomi Gilens, Katherine Haas, Brian Hauss, Mike Katz-Lacabe, Doug Klunder, Mica Moore, Sejal Singh, Jay Stanley, Bennett Stein, Nathan Freed Wessler, Ben Wizner, and Noa Yachot. Thanks also to the participants in the NYU Technology Law and Policy Clinic, and professor Jason Schultz, for their valuable feedback.

The ACLU would like to thank the following affiliates for participating in this multi-state coordinated public records request: Alaska, Arizona, Northern California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Iowa, Kansas/W. Missouri, Kentucky, Louisiana, Maryland, Massachusetts, Minnesota, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, D.C., and Wyoming.

ACLU
AMERICAN CIVIL LIBERTIES UNION