Themis: Research Journal of Justice Studies and Forensic Science

Volume 3 *Themis: Research Journal of Justice Studies and Forensic Science*, Spring 2015

Article 4

5-2015

The Surveillance State: Do License Plate Readers Impinge Upon Americans' Civil Liberties?

Jourdin Hermann
San Jose State University

Follow this and additional works at: <https://scholarworks.sjsu.edu/themis>

Part of the [Civil Rights and Discrimination Commons](#), [Criminology and Criminal Justice Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Hermann, Jourdin (2015) "The Surveillance State: Do License Plate Readers Impinge Upon Americans' Civil Liberties?," *Themis: Research Journal of Justice Studies and Forensic Science*: Vol. 3 , Article 4. <https://doi.org/10.31979/THEMIS.2015.0304> <https://scholarworks.sjsu.edu/themis/vol3/iss1/4>

This Peer-Reviewed Article is brought to you for free and open access by the Justice Studies at SJSU ScholarWorks. It has been accepted for inclusion in Themis: Research Journal of Justice Studies and Forensic Science by an authorized editor of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

The Surveillance State: Do License Plate Readers Impinge Upon Americans' Civil Liberties?

Abstract

The boundaries that delineate public from private sphere have challenged our political system's foundations since its origination. License plate readers (LPRs), a tool used by law enforcement and private businesses, cause citizens and their government to question the criteria separating public and private information. While police and repossession agencies contend that license plate readers aid their work, the American Civil Liberties Union (ACLU) argues that surveillance equipment interferes with an individual's right to privacy. Addressing such privacy concerns requires the public to hold its government accountable by petitioning for limits on LPR use and data retention. LPRs also pose unique threats to public administration. Placing this technology into the hands of public and private interests without informing constituents hinders government accountability. Even though LPRs help police maintain a cost-effective way to handle crime, the United States' federalist structure prevents uniform regulations at local, state, and federal levels. Politics pit those favoring big government against supporters of limited government; thus, creating deadlocks on the issue of LPRs violating an individual's privacy. LPRs ultimately provide a new opportunity to reopen age-old debates within the fields of political science and public administration.

Keywords

license plate readers, surveillance, individual privacy

The Surveillance State: Do License Plate Readers Impinge upon Americans' Civil Liberties?

Jourdin Hermann

Abstract

The boundaries that delineate public from private sphere have challenged our political system's foundations since its origination. License plate readers (LPRs), a tool used by law enforcement and private businesses, cause citizens and their government to question the criteria separating public and private information. While police and repossession agencies contend that license plate readers aid their work, the American Civil Liberties Union (ACLU) argues that surveillance equipment interferes with an individual's right to privacy. Addressing such privacy concerns requires the public to hold its government accountable by petitioning for limits on LPR use and data retention. LPRs also pose unique threats to public administration. Placing this technology into the hands of public and private interests without informing constituents hinders government accountability. Even though LPRs help police maintain a cost-effective way to handle crime, the United States' federalist structure prevents uniform regulations at local, state, and federal levels. Politics pit those favoring big government against supporters of limited government; thus, creating deadlocks on the issue of LPRs violating an individual's privacy. LPRs ultimately provide a new opportunity to reopen age-old debates within the fields of political science and public administration.

THEMIS

Introduction

As technology proliferates around us, society must question the definition of privacy. People now streamline life's mundane tasks by filing taxes and scheduling appointments for the DMV online, but these privileges come with a price, as vast amounts of individuals personal data accumulate in remote databases. One form of technology, known as license plate readers (LPRs), presents a significant challenge to both the public and government. This complex system tracks vehicle locations and stores the information in a database. Although this method of surveillance is widely used across the country, most people do not know of its existence, since public debate rarely precedes its implementation (Anthes, 2012; Gordon & Wolf, 2007; Klein & White, 2011). After the American Civil Liberties Union (ACLU) published its report entitled *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, a broader discussion began to address citizen's privacy concerns.

The primary issue regarding LPRs focuses on the differentiation between public and private information. Secondary questions arise around access; people need to ask their government which entities see this data and for how long (ACLU, 2013; Gordon & Wolf, 2007; Klein & White, 2011). Three overarching themes characterize the study of public administration: politics, performance, and accountability (Kettl, 2015). The controversy surrounding LPRs is important to the study of public administration, because many different aspects of the topic relate to themes in several major ways. First, neglecting to inform the public of new LPR usage voids the ideal of government transparency. Second, public and private entities vying for the rights to LPR databases blur clear delineations of

authority. Third, the different rules regulating LPRs at all three levels of government show how the United States' federalist structure makes uniform laws difficult to attain. Fourth, license plate scanners serve as an effective implementation method for the law enforcement arm of public administration. Fifth, representation of LPRs as a surveillance tool increases the masses' fear of big government. Although LPRs provide police with helpful information to catch criminals, they simultaneously jeopardize the accountability, performance, and politics of public administration; thus, form a need for regulation that controls the accessibility and maintenance of LPR data.

Background

LPRs utilize a combination of cameras and computer software to achieve their results. Cameras easily mount to either stationary or mobile locations where they take pictures of all passing cars (ACLU, 2013; Anthes, 2012; Gordon & Wolf, 2007). Software subsequently converts the photographs, making the alphanumeric string that comprises each license plate digitally readable (ACLU, 2013; Anthes, 2012; Gordon & Wolf, 2007). Data is then compiled into a system that compares the collected license plate images against various databases, which match trigger alerts for law enforcement to inspect more closely (ACLU, 2013; Anthes, 2012; Gordon & Wolf, 2007). Police often use the National Crime Information Center (NCIC) to track the movements of kidnappers and other criminals fleeing from the law (ACLU, 2013; Gordon & Wolf, 2007). The cameras and accompanying software also allow law enforcement officials to quickly locate stolen cars (Angwin & Valentino-DeVries, 2012; Gordon & Wolf, 2007; Klein & White, 2011; Sullivan, 2013). Even though police represent a large demographic of LPR users,

THEMIS

many others in public and private sectors have started employing LPRs to make their jobs easier.

Responsibilities of law enforcement typically reside with state or local government branches, but the federal government also recognizes the advantages afforded by LPRs. The Internal Revenue Service (IRS) uses the technology to cash in on delinquent tax payments (Klein & White, 2011; Nakashima, 2014). Other government agencies such as the Drug Enforcement Administration (DEA) and Immigration and Customs Enforcement (ICE) also capitalize on the wealth of information that LPRs offer to arrest criminals on their wanted lists (ACLU, 2013; Nakashima, 2014). Repossession companies, known as the “repo” guys, created most of the private sector demand for LPRs by incorporating them into their business models (ACLU, 2013; Angwin & Valentino-DeVries, 2012; Orr, 2014). MVTrac, a private company, charges the repossession business Final Notice & Recovery LLC to install MVTrac’s cameras on its repo agents’ cars (Angwin & Valentino-DeVries, 2012). Armed with the LPR technology, Final Notice & Recovery LLC deploys a “team of ‘night spotters,’ who drive after dark, scanning plates” hoping to repossess vehicles that borrowers use as collateral (Angwin & Valentino-DeVries, 2012). This accumulation of personal data by private companies prompts concerned constituents in many states to critically assess the rules in place that govern this technology.

Lacking guidance from the federal government, law enforcement officials are left to devise their own strategies for guarding LPR data. In fact, “scant legal precedent” exists so far on LPRs, and data retention policies differ significantly across state borders (Crump, 2013; Klein & White, 2011). For example, Maine exemplifies the ACLU ideal by restricting camera use

solely to state law enforcement, which leaves no access for private companies (Bohm, 2013). Some jurisdictions, such as the Minnesota State Patrol, delete their scans after 48 hours (ACLU, 2013). Even with regulations in place, one finds that different police departments within the same state do not always share identical procedures (Sullivan, 2013). California embodies both state and departmental discrepancies. Los Angeles keeps possession of its data for two years, while Milpitas stores license plate images indefinitely (ACLU, 2013). In an effort to promote uniformity across the state, a bill was proposed in the California Senate permitting 60-day availability to license plate databases under two conditions: law enforcement must be the only recipient of LPR information kept by private companies and search warrants must accompany police request for access (Schulz, 2012). The proposed bill ultimately failed under stress from powerful lobbyists. Police fought for the warrantless use of private companies' information, and businesses fought for the right to freely compile their databases with ones produced by the police (Schulz, 2012). Despite this bill's inability to create lasting legislation, privacy concerns still prevail and raise questions about the wide authority granted to our law enforcement officials.

The Various Perspectives

In the debate over LPRs, an alliance of private companies and law enforcement officials attempt to counteract the ACLU's demands. Police argue that their line of work necessitates steady availability of the cameras, software, and databases for several purposes. For example, LPR technology serves as an enforcement device and an "investigative tool" (Klein & White, 2011). The data reveals a car's location at a certain date and time, thus providing evidence of any traffic law

THEMIS

violation(s) (ACLU, 2013; Gordon & Wolf, 2007). LPRs also allow police to collect payments for the resultant fines if they become delinquent, since LPRs alert police once they pass a car with outstanding tickets (Angwin & Valentino-DeVries, 2012). The cameras can also potentially help police prevent crime before it occurs by giving them a set of eyes in locations most prone to violence. One example proposes that nightclubs benefit from the aid of LPRs since police can see which patrons enter the parking lot and are able to judge if violence might ensue (Klein & White, 2011).

Evidence seems to support the technology's effectiveness and the police's point of view on LPRs. San Leandro, California has only one LPR atop of a police car, yet it enabled police to catch a Las Vegas man suspected of homicide (Angwin & Valentino-DeVries, 2012). Maryland finds similar results with its incorporation of LPRs. Over 800 "serious traffic citations" and "the apprehension of 180 people for crimes including stolen autos or license plates" were made possible through the use of LPRs (Timberg, 2013). Police possess two persuasive arguments in their crusade for continued access to the technology. Some law enforcement officials have been quoted in favor of LPRs, saying "the data [should be kept] as long as possible, because it...provide[s] a rich and enduring data set for investigations down the line" (Roberts, as cited in Timberg, 2013, para. 7). Law enforcement also reminds citizens that their job necessarily entails access to other personal information like Social Security numbers (Klein & White, 2011). Rules usually prevent police from abusing the privileged information, but private companies are often exempt from the same type of monitoring.

The repossession companies utilizing LPRs perform far less duties than the police, but they seem to pose a much more alarming threat to one's privacy. Two companies dominate license plate data collection in the private sector: MVTrac and Digital Recognition Network (DRN) (ACLU, 2013; Angwin & Valentino-DeVries, 2012). Todd Hodnett originally formed DRN as a tool for repossession agencies, but he later decided to collaborate with police (Orr, 2014). The DRN eventually partnered with Vigilant Solutions to create the National Vehicle Location Service (NVLS); DRN feeds its data into NVLS while Vigilant Solutions runs technological operations (ACLU, 2013; Orr, 2014). NVLS does not solely rely on DRN's data, since several private companies and law enforcement groups contribute to the overall product (ACLU, 2013). Private businesses greatly improve the databases with their own collection efforts, but problems arise when money starts to separate the public sector from the private. The DRN entitles police to freely look at the company's aggregate data supply on a limited basis; unlimited access comes with a fee (Orr, 2014). MVTrac's owner holds onto his LPR data since "[e]very day it just gets more valuable because [they] collect more information" (Angwin & Valentino-DeVries, 2012). Police and repossession agencies seem to have struck the right balance for now. If demand increases, market pressures might encourage these private companies to charge higher prices for their services, leading to issues of accountability in public and private spheres.

The ACLU starkly opposes the police and repossession agencies' current use of LPR technology. To be clear, the ACLU does acknowledge that LPRs essentially pose no harm when used to capture criminals (with the proper warrant) or to retrieve stolen vehicles (Crump, 2013). ACLU's problem originates with

THEMIS

the long retention spans and the inclusion of the private sector in matters of what they argue to be private information. Even though statistics show promising results of the license plate readers' ability to help solve crime, the numbers really portray a different picture when viewed through a broader context. The ACLU found that less than 1% of license plate scans actually register vehicles inhabited by wanted drivers, with an even smaller number leading to arrests (ACLU, 2013). Since most of the data compiles information on the innocent, the ACLU believes that such monitoring inevitably alters people's behaviors. LPRs track car movements and thus place people at certain locations such as church, political protests, or drug addiction facilities (Moore, 2013). When people experience feelings of surveillance, they often stop engaging in perfectly legal activities for fear of how those watching might perceive their actions (Moore, 2013). Without regulation, the ACLU insists that the data collection system can be abused for malevolent practices, such as tracking a spouse or a workplace rival (ACLU, 2013). The ACLU eventually concludes that both private companies and the police may continue using LPRs if they delete their stored scans within a couple of days or weeks (ACLU, 2013). Law enforcement must present "reasonable suspicion" of a crime to gain database access, and they must share data transparently with other entities (ACLU, 2013). Improvements in regulation, such as these, can ease the public mindset by allowing people to follow the whereabouts of their private information.

Analysis of the Key Components

LPRs come with various pros and cons that encourage debate between citizens and their government. The main issue causing controversy questions whether license plates constitute

public or private information. Many believe that no one can assume privacy on a busy public street since everyone there bears witness to each other's actions (Angwin & Valentino-DeVries, 2012; Bravin, 2012; Klein & White, 2011). The same circumstances characterize the use of LPRs. A Supreme Court decision regarding GPS tracking concluded that law enforcement's use of such digital surveillance methods must include a warrant (Liptak, 2012). It seems that for the moment LPR data will be considered private information.

Despite this new development, government accountability still faces challenges from LPRs. The initial absence of public debate on the topic essentially allowed law enforcement to use the technology with few repercussions. Accountability requires that people know about situations in which the government is collecting personal information on their whereabouts. Law enforcement must inform the public of its LPR use; however, the actual camera location cannot be disclosed. Telling people precisely where the LPRs have been placed might just decrease criminal activity in those areas, prompting violations to occur elsewhere. Allowing both police and repossession agencies the ability to use license plate databases also threatens accountability, since the public sector often has stricter regulations than the private sphere. Cooperation between the two sectors blurs positions of authority; it is unclear who is really in charge of the databases. The simple answer entails consolidation of the information into either the hands of law enforcement or repo men, but this fails to consider the significance of aggregate data. Combining two entities provides a much larger supply of resources than the two could ever accumulate separately. The issue thus reveals itself as a much

THEMIS

more delicate situation once all the vested interests come into play.

LPRs similarly affect the performance and politics of public administration. The fragmented structure produced by federalism leads to obstacles in the regulation of LPRs within and between the multiple levels of government. Now that the local, state, and federal government branches employ LPR technology, uniform standards concerning the data's usage should be implemented. Universal regulations across geographic boundaries ensure that government effectively delivers services by eliminating confusion regarding the legal use of LPRs.

Certain aspects of LPR databases actually work to improve performance by increasing cost-effectiveness and coordination. Stationing cameras on police cars and fixed locations increases the amount of eyes on crime without adding to a department's personnel. LPRs ability to serve enforcement and investigative needs provides large cost benefits, since the technology can perform work that people would normally have to be paid for. Some states, like Vermont, allow their police departments to compile data into a statewide database (Bohm, 2013). This type of data sharing augments coordination because each department has access to the same data, thus no police department holds an advantage over any other.

Politics functions to initiate much of the debate concerning LPRs. The largest predicament asks about the role of government, mainly questioning whether it should be big or limited. LPR imaging as a method of surveillance causes many to envision the rise of a large and intrusive government. Larger governments have the resources to provide its citizens with more economic and physical security. The Founding Fathers left the proper size of government up to the discretion of future

generations, but it continues to plague public administration to this day.

Conclusion

The widespread use of LPRs ushers in a new era of possibilities and restrictions. LPRs streamline law enforcement officials' duties as they locate criminals quicker and easier than before, while private repossession companies increase their profits by selling their license plate data to entities wishing to collect payments from delinquent borrowers. Even with these improvements, several issues surround the new technology. Citizens wonder if their license plates count as private information and, if so, what can be done to protect them? Safeguarding the data requires standards that impose limits on who can view the information and for how long. These questions directly relate to various lines of inquiry within public administration. The implementation of LPRs initially neglected public debate, leading citizens to question their relationship to government. Private companies capitalize on the innovation by redirecting it towards the private business's bottom line of profit, but the inclusion of the private sector blurs accountability. Government performance becomes impaired when federalism prevents the creation of universal regulations. Despite these challenges, LPRs do present the police with a cost-saving approach to coordination. LPRs embody the age-old debate that pits big government against limited government, causing proponents from each side to shape the politics of public administration. Government faces a unique challenge from LPRs as it contemplates the issues of politics, performance, and accountability raised by the use of this new technology. Now license plates hold much more information than the mixture of characters imprinted upon their surface.

THEMIS

References

- American Civil Liberties Union. (2013). You are being tracked: How license plate readers are being used to record Americans' movements. Retrieved from <https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record>
- Angwin, J., & Valentino-DeVries, J. (2012). New tracking frontier: Your license plates. *The Wall Street Journal*. Retrieved from <http://online.wsj.com/articles/SB10000872396390443995604578004723603576296>
- Anthes, G. (2012). Vehicle license plates and surveillance. *Communications of the ACM*, 55(10), 16. Retrieved from <http://cacm.acm.org/magazines/2012/10>
- Bohm, A. (2013). 'Limited only by the imagination': The need for legal limits on license plate reader use. *American Civil Liberties Union*. Retrieved from <https://www.aclu.org/blog/technology-and-liberty-national-security/limited-only-imagination-need-legal-limits-license>
- Bravin, J. (2012). Justices rein in police on GPS trackers. *The Wall Street Journal*. Retrieved from <http://online.wsj.com/articles/SB10001424052970203806504577178811800873358>
- Crump, C. (2013). Police documents on license plate scanners reveal mass tracking. *American Civil Liberties Union*. Retrieved from <https://www.aclu.org/blog/technology-and-liberty-national-security/police-documents-license-plate-scanners-reveal-mass>

- Gordon, A., & Wolf, R. (2007). License plate recognition technology: Innovation in law enforcement use. *FBI Law Enforcement Bulletin*, 76(3), 8-13. Retrieved from <http://leb.fbi.gov/2007-pdfs/leb-march-2007>
- Kettl, D. F. (2015). *Politics of the administrative process*. (6th ed.) Los Angeles, CA: CQ Press.
- Klein, A., & White, J. (2011). License plate readers: A useful tool for police comes with privacy concerns. *The Washington Post*. Retrieved from http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html
- Liptak, A. (2012). Justices say GPS tracker violated privacy rights. *The New York Times*. Retrieved from http://www.nytimes.com/2012/01/24/us/police-use-of-gps-is-ruled-unconstitutional.html?pagewanted=all&_r=0
- Moore, M., & Stein, B. (2013). The chilling effects of license-plate location tracking. *American Civil Liberties Union*. Retrieved from <https://www.aclu.org/blog/technology-and-liberty-national-security/chilling-effects-license-plate-location-tracking>
- Nakashima, E. (2014). ICE twice breached privacy policy with license-plate database. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/ice-twice-breached-privacy-policy-with-license-plate-database/2014/10/29/df3a8e6c-5096-11e4-8c24-487e92bc997b_story.html
- Orr, S. (2014, November 2). License plate data raises privacy concerns. *The Washington Times*. Retrieved from

<http://www.washingtontimes.com/news/2014/nov/2/license-plate-data-raises-privacy-concerns/?page=all>

Schulz, G.W. (2012). Police, lobbyists defeat attempt to limit license-plate scanners. *California Watch*. Retrieved from <http://californiawatch.org/dailyreport/police-lobbyists-defeat-attempt-limit-license-plate-scanners-16699>

Sullivan, M. (2013). License-plate scanning: The inside story. *PC World*, 31(10), 15-17.

Timberg, C. (2013). License-plate cameras track millions of Americans. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/license-plate-cameras-track-millions-of-americans/2013/07/17/40410cd0-ee47-11e2-bed3-b9b6fe264871_story.html

Jourdin Hermann expects to graduate with her bachelor's degree in Political Science from San Jose State University in May 2015. She will also graduate with minors in Radio, Television, and Film and Women, Gender, and Sexuality Studies. Her previous work for Themis includes "No One Cried for Help: The Integration of Groupthink into Modern Rape Culture." Jourdin is a member of both the interdisciplinary Phi Kappa Phi Honor Society and the Pi Sigma Alpha Political Science Honor Society. In addition to her scholastic endeavors, Jourdin enjoys working at her internship with the Silicon Valley Council of Nonprofits where she helps advocate for public policy on behalf of the organization's members. When not engaging in those activities, she can be found watching Shark Tank and Law and Order: SVU.