Automated License Plate Recognition Technology: Social and Security Implications
Jordan Nichols
IT 103- 001
October, 6 2013

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/honor-code/. I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site.
Automated License Plate Recognition Technology: Social and Security Implications

Introduction

Automated License Plate Recognition (ALPR) systems use cameras to capture images of license plates and other related information. ALPR technology has many potential uses. However, despite its various applications, this technology is almost exclusively thought of as a tool for law enforcement officers. Here, we will adopt this prevailing focus of ALPR issues from a law enforcement lens. ALPR technology is emerging as the next step in automating basic police functions in many departments across the world as agencies employ these systems to increase police performance and efficiency at crime detection and criminal apprehension. As the use of ALPR technology becomes more prevalent, many privacy advocates are urging law enforcement agencies to consider the social implications introduced by this kind of surveillance technology. The following discussion evaluates ALPR technology with regards to its legal, ethical, security and social implications.

Background

ALPR systems combine high-speed cameras with sophisticated algorithms which convert images of license plates into data that can be read and processed by computers. That data is then evaluated against a pre-loaded database, or “hot list,” of license plates which are of interest to law enforcement (Lum, Merola, Willis and Cave, 2010). In addition to visible light cameras, many ALPR systems also employ infrared cameras to compensate for factors such as light conditions, headlight glare, and harsh environmental conditions that might inhibit a camera’s ability to capture license plate images (IACP, 2009).

ALPR cameras can be utilized in a variety of circumstances and may be presented as fixed, mobile, or portable units. The combination of these assists in the detection and pursuit of
vehicles which are of interest to law enforcement. Fixed ALPR units provide auxiliary support to officers because their use does not require law enforcement personnel to be in the vicinity at the time of an incident. Fixed ALPR units are most often utilized in a jurisdiction’s most frequented points of ingress and egress and can be accessed after a crime has occurred to scan a point for vehicles matching a suspect’s description. Mobile ALPR units are located on law enforcement vehicles and have the potential ability to capture up to 3,000 license plates per hour (Gaumont and Babineau, 2008). Most patrol cars that are outfitted with ALPR systems contain four to six cameras operating to capture images of different angels of the vehicle and are linked to a CAD SYSTEM inside of the patrol car. As the name infers, portable ALPR units can be shared across different vehicles and most often have implications for more covert data capturing.

Images capture by ALPR systems may be “contextualized” to include non-electronic information in addition to electronic information. Contextualization may include images of license plates in addition to images of the vehicle’s make and model, occupants, and other distinguishing features such as bumper stickers or damage. GPS coordinates or other location information such as the date and time of observation are also often used to contextualize an image.

**Potential benefits**

This technology has already begun realizing its potential as a tool for law enforcement. Though not yet systematically evaluated, ALPR is thought to be a strong deterrent to crime and increase the apprehension of suspects in an investigation. It also increases public safety by leading to better information sharing through the use of hot lists and increasing public confidence in a department as it reduces opportunities for bias. Each license plate that passes through the
frame of the ALPR cameras is scanned and searched, reducing situations where race or other discriminatory factors might bias an officer’s suspicions and subsequent inquiries, thereby insulating departments from profiling blowback for traffic offenses.

It is also significant to note that though the crime application of the tool dominates, actors other than the state have access to ALPR and may employ it for their own personal security. More and more loss prevention departments in big businesses are finding it worthwhile to purchase and employ this technology despite its restrictive cost, which is around $25,000 per unit. ALPR can benefit business by enhancing their security and insulating them from complaints. Many law enforcement departments have found the technology to be useful in reducing civil complaints against biased judgments to pursue a vehicle.

**Legal and ethical issues**

As with many new technologies, legal and ethical arguments are most often raised over the storage and potential secondary uses of the information obtained through ALPR, rather than the data’s initial collection. Privacy advocates have chosen the line between active and historical ALPR data as the focus of their arguments. Active ALPR data is that information which is provided to an officer immediately when an ALPR system identifies a license plate as a match to one on a hot list. This ‘hit’ is active data because the officer is likely to take immediate action.

Historical ALPR data is contained within a database of previously collected ALPR information. Historical ALPR data is considered passive because it is not identified for immediate action, but is stored for future use. Many privacy advocates cite the secondary uses associated with historical ALPR data as most concerning for potential misuse or accidental disclosure, including the potential to track an individual’s movements over a long period of time.
and identify personal, but not protected, information such as where they shop and where their children may go to school. Though the contextualization of ALRP images may include the vehicle’s occupants, the current ALPR systems employed by law enforcement agencies are not designed to capture this type of information. Additionally, images of occupants are very rarely used for identification; instead the focus is on confirmation. Therefore a reasonable suspicion is present before any use of personally identifiable information from ALPR data is attempted.

Law enforcement agencies respond to such criticism with the argument that ALPR simply automated the system that the public has already accepted as necessary for the efficient conduct of law enforcement. The IACP succinctly writes (2009) that “ALPR systems simply improve the accessibility of information that is already publicly visible and make it available for analysis and appropriate dissemination.” From a legal standpoint, the use of ALPR does not fall under the category of unreasonable search and seizure because it only picks up information that is publically exposed.

**Security concerns**

From a government standpoint, the use of this technology should alleviate security concerns because it makes us safer by allowing law enforcement to apprehend suspected criminals faster. Additionally, many law enforcement officers and other commentators believe that the use of ALPR has a deterrent effect on crime, actually reducing criminality and victimization instead of simply aiding the investigative process after victimization has already occurred.

From a privacy advocate’s standpoint, we may be putting our security and liberty in jeopardy by allowing the government to build databases with our locations and accompanying
images. Though this message may be agreed upon by many citizens, fewer find that this possibility is worth abandoning ALPR technology. As with many other government technologies, despite the potential for misuse there is a wide recognition of the benefits and a commonly held understanding that increased security sometimes requires us to relinquish some of our privacy. The use of ALPR technology seems to be an instance where society has mostly agreed that its security benefits are worth the privacy risks it imposes on citizens.

Social problems

Some of the social concerns for the use of technology include a fear that citizens will develop a mistrust of law enforcement or that they will change their habits and personal development as a result of the “tracking” and “mapping” potential of ALPR. The IACP (2009) recognizes that “retaining certain types of information indefinitely can be a form of undesirable social control that can prevent people from engaging in activities that further their own self-development, and inhibit individuals from associating with others, which is sometimes critical for the promotion of free expression” and we can subsequently hope that they are assessing what they can to minimize this potential, negative effect.

Further required research

A systematic evaluation of ALPR use in police agencies in the United States should be conducted to determine the extent to which ALPR is utilized as well as to estimate the value of ALPR as a deterrent and asset for the apprehension of individuals in investigations. The justifications for the use of this technology, though both logical and backed by anecdotal evidence, have not been secured by a systematic scientific evaluation. Additionally, more
research should be conducted on ALPR accuracy. IACP (2009) observed, “For maximum effectiveness, ALPR systems must be properly configured to recognize the design and layout of plates most likely to be encountered in the area of operation.” Steps must be taken to reduce inefficiencies and mistakes caused by design and other factors straining the ability ALPR systems to recognize and interpret data points.

**Conclusion**

ALPR technology has emerged as the next step in automatizing basic police functions in law enforcement agencies across the United States to increase police performance and efficiency at crime detection and criminal apprehension. Despite some concerns over the technology’s application, many remain excited about this new tool and its potential to keep our communities safer. The arguments aforementioned in this paper illustrate an understanding that while there are some concerns over the expanded use of ALPR, it is one of the best tools that law enforcement has at its disposal to increase public safety without raising time-concerns, risking public safety or introducing bias from selectively targeting certain vehicles and vehicle operators.

These arguments strongly suggest that the privacy tradeoff, though a valid concern, does not extend significantly past the allowances that are already in place for law enforcement to conduct their public safety mission and that the increase in security makes these risks worthwhile. However, ALPR researchers and law enforcement officials should continue working on developing ways to improve this technology and reduce the impact of historical ALPR data on citizen’s privacy, both perceived and actualized. As this technology continues to spread across United States’ law enforcement agencies, it will be interesting to see what other
capabilities are introduced to the technology and whether the management of ALPR use is left to individual agencies or becomes regulated by a national entity in the future.
Bibliography


This brief, one-year-old opinion by Kade Crockford, the Director of the American Civil Liberties Union of Massachusetts Technology for Liberty Project, is written from the bias of a privacy advocate, which provides a useful contrast to the official law enforcement sources used in this paper. Though the author’s perception of law enforcement’s intent for this technology is not based in fact, it does bring up many points that are useful to our consideration of ALPR technology. This article is uniquely useful when seeking to describe the business aspect of ALPR because it was the first source the author found which addressed the business side of ALPR proliferation. Though the overarching points of the article are accurate, some of the supporting assertions may be tainted by bias. Kade Crockford’s arguments remain, however, relevant and timely to our discussion of ALPR and allow us to more fully evaluate the costs and benefits of this new technology.


This source enhances the quality of this paper because it lends an international perspective on the capability and use of ALPR technology. This short article, accepted into *The Police Chief*, a well-known policing journal sponsored by the International Association of Chiefs of Police, broadens its reader’s basic understanding of ALPR technology by providing a brief overview of its history, use, and a short discussion of the applications and benefits of ALPR systems. This article was published in 2008 and, as such, some of its numerical yields could be quite different today. This paper, however, utilized this article’s more general assertions, which remain current and accurate. The purpose of this information is to inform the public, and other police agencies, of the potential benefits of employing ALPR technology and, most likely, defend the technology against some of the reproaches made by privacy advocates.


The IACP’s privacy impact report was an excellent source for background and operation information of ALPR as well as the discussion on legal, ethical and social implications of this technology’s utilization by law enforcement agencies. Written in 2009, the broader ideas and arguments are still relevant today and inform the reader of both strengths and weaknesses of the technology, though the emphasis is on strengths. This source, from a very well-known and
credible law enforcement authority, may project a bias in the favor of law enforcement but does a fair job recognizing that bias and addressing concerns that are not its own.


This source is current and uniquely relevant to this paper because it is the only source that could be found which included an actual evaluation of the technology’s use. It was published in 2010 by a team of researchers from the Center for Evidence-Based Crime Policy at George Mason University and was written for the purpose of informing police practitioners and policing scholars of the effectiveness of ALPR. It is a very accurate source backed by evidence. Its extensive bibliography provided a great point from which I could obtain leads for other great sources for this paper.


The report listed above was a good reference source for this paper. Though not directly related to my exploration of License Plate Recognition Systems, the information contained in the aforementioned report allowed for the development of a thorough reference point from which the ethical and legal implications of LRP technology could be evaluated. The source is only three years old and speaks from a high authority, as the paper was sponsored by the U.S. Department of Commerce’s National Institute of Standards and Technology. Though the NIST’s sponsorship is clearly presented on the cover page of the report, the qualification of this paper to set definitions of privacy and extrapolate best practices can also be divined more simply from its “.gov” URL. The reliability of the content is very strong. The definitions provided in this report are timely, come from a reliable authority, and coincide with the logical, but often unarticulated, perceptions of privacy issues and terms in the United States today. This report did not introduce new information, but rather provided an opportunity for a governmental authority to articulate privacy definitions and concerns, long-experienced by U.S. citizens but not yet expressed systematically in a manner which is conducive to discussions for progress. This source allowed me to base my discussion of the ethical and legal implications of ALPR technology on reliable definitions for terms of privacy and information which is considered personally identifiable information.