License tag readers: issues and constitutional concerns case study example

Law, Criminal Justice

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

(Institute/University)

Introduction

A seldom noted observation device geared to monitor the movements of every passing motorist is rapidly spreading on America’s thoroughfares. “ Automatic license plate readers” that are placed on police cruisers or on stationary locations such as bridges-utilize small high speed cameras to take pictures of thousands of license plates every minute. The data taken by the readers-inclusive of the plate of the vehicle, the date, time and area of the scanning-is then gathered and at times lumped together into regional data pools. As a result of these activities, innocent motorists have their private information taken and pooled into these government databases (American Civil Liberties Union, 2015, p. 1).

Federal officials are looking to widen the application of “ license tag readers”

that permits police officers to check license plate. The readers allow police officers to determine if the cars were stolen or are being used by known or suspected extremists. At present, Prince William County police officers have used the readers to identify and reclaim 10 stolen cars resulting in the arrest and prosecution of four felons in the time frame that the readers have been in use. Homeland Security has asked for funding to purchase additional readers and be distributed across Northern Virginia with the objective of centering on cases of terrorism (Sherfinski, 2008, p. 1).

The Homeland Department is looking to acquire information regarding the location millions of Americans and their driving itineraries. Under the “ Privacy Impact Assessment” of the department, Immigration and Customs Enforcement (ICE) policy makers decided to “ procure the services of a commercial vendor of LPR information.” Even though there have been numerous protests against the policy, the department has paid nothing more than token attention regarding the use of the readers and gives some enhancements on the government’s unfettered use of the technology. The improvements, however, do not give any sort of redress to growing fears of possible abuse of technology. Homeland Security officials aborted a plan to access a US-wide after the discovery of the plan triggered a social outrage. The range that the government wanted to derive from the national directory stunned the public as well as lawmakers; more than two billion data gathering points, rising at 70 million pictures per month shared and distributed from police and law enforcement agencies across the United States (Stanley, Stein, 2015, p. 1).

In the research of civil rights watchdog American Civil Liberties Union

(ACLU), these readers are gaining ground in other parts of the United States as well. California Highway Patrol elements as well as other Northern California law enforcement agencies are now able to monitor the movements of millions of California motorists and citizens and even collaborate with Federal agencies to develop a national database using the information collated by these readers (Cagle, 2013, p. 1).

Constitutional implications

In a report by the ACLU, the group stated that the United States Federal Bureau of Investigation (FBI) is the lead agency in the deployment of these surveillance technologies in a number of its satellite offices. The slew of documents pointing to this fact was obtained by the group with “ right to information” statutes. In addition, the report also disclosed that the program was aborted owing to privacy concerns hounding the policy (Pilkington, 2015, p. 1).

The use of these readers, according to the statement of civil rights guardian Rutherford Institute, is not only disturbing; it is also in violation of the United States Constitution, particularly the Fourth Amendment. These mechanized license plate readers can collect the data from cars passing at a certain location, and give the exact location of approximately 1, 800 vehicles per minute. The data is then conveyed to a main data storage facility that can compares Department of Motor Vehicle (DMV) records as well as other recordings where the vehicle passed through.

The Fourth Amendment bars capricious searches and seizures, and these activities can only be accomplished with the acquisition of a warrant similar

to the proffer against the national espionage policy of the government. According to Rutherford Institute head John Whitehead, the Fourth Amendment is unequivocal about the mandate that any search and seizure action must only be done with a warrant. Aside from the Fourth, the program threatens the liberties stipulated in the First Amendment; with the information gathered, these can be used against the person if, for example, at political protest rallies. What exacerbates the issue is that the entity that captured the photos, the Virginia State Police, took the photos at political events for the President and Sarah Palin. Surveillance pictures taken at such events can prove to be an issue for people who engage the services of clinicians or political figures that have substance abuse issues who is looking for assistance. In short, Whitehead avers that the information can be used against these individuals in the future.

The use of the license plate reader technology is not only within the borders of the Old Dominion. In a national poll conducted by the Police Executive Research Forum, 7 out of 10 police organizations disclosed using the technology; 8 out of 10 agencies reported plans on expanding the use of the technology within their jurisdictions. Law enforcement agencies proffer that the readers help in reducing criminality in their areas, and it can be stated that the readers have helped in reducing criminality. In Maryland, for example, out of one million license plates that were scanned, only a small fraction of these were connected to serious offenses, as per the report of the ACLU. Nevertheless, Whitehead proffers that all the technology is accomplishing is stalking innocent people (Watson, 2014, p. 1).

The significance of the readers in the crime eradication initiative is clear. The

systems continually run unhindered taking pictures and compare the images to the information in the database in split seconds. When a “ match” is made, the system gives off an alarm, and the computer monitor displays the plate of the vehicle, the known owner of the vehicle, and the suspected criminal action where the vehicle is suspected of participating in as well as the direction of the vehicle at the time that the image was captured. Nevertheless, representatives of the American Civil Liberties Union, there is significant worry on how the information is saved and secured. In addition, there are misgivings that a number of police organizations that use the services of private entities rather than public agencies to save the information (Cook, 2012, p. 1).

There are jurisdictions that are taking action against the use of the technology in their areas. Utah adopted a law that circumscribes opportunities for snapping a picture and at the same time using technology to examine the picture. The “ Utah Automatic License Plate Reader (ALPR) law ban the use of mechanized “ high speed cameras” to snap pictures of license plates within the state of the Utah; this particular issue may have wide reaching effects across the United States as more than 20 jurisdictions are in the process of assessing legislative proposals that limit the use of the technology in both private and law enforcement settings. Moreover, five areas have already adopted laws that are the same or comparable to Utah’s law.

The constitutional dilemma here is not with the citizenry, but with the companies that are implementing the programs in Utah. According to Digital Recognition Network, Inc. (DRN), and Vigilant Solutions, Inc. (Vigilant), the

Utah law summarily bans a protected action that is legal in every other scenario and infringes on the companies' First Amendment rights. According to the companies, the law violates the right against free speech and inflicts on the companies " irreparable and imminent injury." According to the companies, snapping and sharing a photo is a constitutionally protected act under the operation of the First Amendment. A state such as Utah cannot definitively state that taking a picture violates a person's right to privacy. License plates are public by character and do not have any critical or private data (Vigilant Solutions, 2015, p. 1).

However, there are concerns that the images taken by the scanners may be more than just the figures on a car's license plates. A California citizen supported by the ACLU asked the San Leandro Police Department to release to him the photos taken by the cameras on the police cruisers. The images revealed more than just the license plates of the car; it clearly identified the man and his daughters as these were getting out of the vehicle. The ACLU stated that aside from police agencies, the United States Drug Enforcement Administration (DEA) is also using the technology to take pictures of the drivers as well as the passengers of the vehicles (Herrera, 2015, p. 1).

The Justice Department, who oversee the operation of the DEA, stated that the program is in full compliance with the tenets of the law. The DEA has strongly stated that the agency is using the readers solely for the purpose of tracking and neutralizing criminal elements and eliminates the flow of narcotics in jurisdictions where there is a high concentration of trafficking activity. However, the use of the readers, according to Senator Patrick Leahy, senior Democrat member on the Senate Judiciary Committee, generates

significant threats to one’s right to privacy, and the fact that the technology is being used in furtherance of the government’s asset confiscation program generates even more concern on the potential effects of the program. In this light, Leahy called for increased transparency on the part of the government agencies and averred that all Americans shouldn’t have to be fearful of being monitored and then stored in a huge government data storage facility.”

Documents acquired by ACLU show that the data gathered by the DEA is then transmitted into its own system and as a result, generate a massive data store that is continually being updated and expanded with the mechanism geared to direct law enforcement personnel to criminals. According to ACLU senior policy specialist Jay Stanley, any data storage facility that gathers location data of average Americans that are not suspected of criminal activity is extremely alarming. The ACLU believes that the use and objective of the program is unjust, and the use of such wide reaching technology can be used in society without so much fanfare. Individuals will digress on the manner that the technology can and should be used; that use must be done in a democratic manner and not done in an arbitrary manner.

In bolstering their case, the DEA stated, basing on internal reports, the program helped in the confiscation of approximately 98 kilos of cocaine, more than 8, 000 kilograms of marijuana, and in the seizure of more than $860, 000. In addition, the program has been linked to the “ Amber Alert” system that helps in locating kidnapped children. However, the activity is increasingly being attacked on allegations that law enforcement officers

have actually confiscated assets even without any proof that the individual committed any criminal offense (Refuge, 2015, p. 1).

Storage and sharing issues

In the findings of the ACLU, law enforcement agencies were rapidly moving towards a policy of storing every piece of information and distributing the information reader-gathered information liberally. The ACLU further argues that the biggest issue of the ALPR mechanisms is the development of data bases with information on motorist information on all motorists that comes into contact with the system and not just the government targets. On a national level, ALPR mechanisms are being engaged in using the ALPR systems to quietly build a database containing millions of license plate data, storing them in “ backend” data base facilities. Though the ACLU does not have an actual gage of the issue, the group knows that legal deletion of the stored information in the database is the exception rather than the rule.

For example, in Georgia, the ACLU used the state’s Open Records Act to file requests from several police agencies in the state as well as the Georgia Emergency Agency. These agencies have basically stonewalled the requests; other chapters of the ACLU have run into similar tactics. As a result of these delaying tactics, the Massachusetts affiliate of the ACLU filed cases against the United States Department of Justice as well as the United States Department of Homeland Security in federal court owing to the continued refusal of the two agencies to disclose any data on the manner that the mechanism gathers information. The Georgia State Patrol has been utilizing the ALPR mechanism since 2004, and according to Lieutenant Kermit Stokes,

who administers the program for the GSP, only he and one other person have access to the stored information and each information byte will ‘ age out’ after a period of six months (Cook, 2012, p. 1).

In 2012, ACLU associates in 38 US jurisdictions as well as Washington released ‘ public records requests” to nearly 600 local as well as state law enforcement agencies and Federal agencies to procure information on the manner that these agencies use the data gathered from the license plate pictures. The ACLU revealed that in response, the organization got more than 26, 000 pages of papers that detail the usage of the information across the United States. The content of the documents reveal a disturbing artwork of a mechanism unleashed on a society without a strong safeguard to protect the rights of the people; moreover, the lack of safety nets against too much intrusion by these mechanisms has resulted in transforming the system into nothing more than a routinely tracking and mass monitoring system (ACLU, 2015, p. 1).

The United States Department of Justice has been silently building a Federal data storage facility to be able to monitor on a real-time basis vehicle movement in the United States. The clandestine information gathering system has the ability to scan and store hundreds of millions of records regarding the personal information of motorists, according to the statements of present and former government officials as well as government papers. The basic objective of the policy, administered by the Drug Enforcement Administration, is to confiscate cars, monies and other resources to counter drug trafficking, in the content of a government report. However, the program’s scope has been widened to include locating cars connected to

other possible criminal offenses. Government policy makers have publicly stated that the government monitors vehicles adjacent to the Mexican border to assist in the war against drugs. What has not been publicly disclosed is that the DEA has extensively worked to expand the scope of the program to encompass the whole United States (The Last Refuge, 2015, p. 1).

The ALPR technology has the capacity to scan thousands of plates in span of one minute. Once the data has been received and stored in the data base, the movements of innocent, law abiding individuals will be held for years on end. Regrettably, the agencies that utilize the technology without any clear cut procedures for the gathered in the course of the operation of these readers. Sans any effective protections, license plate readers, as mentioned earlier, can be used to list down the license plates of militants in a protest action, gather information on a person’s visits to their clinicians, entertainment spots, religious activities, or other personal activities.

The “ small” sample of data collected by a limited number of Northern California police organizations display how easy it will be to track the movement of people using the system. Sadly, there are no state laws on protecting the privacy of individuals whose plates have been recorded. Moreover, many local police agencies do not have specialized policies affording protections as well. Of the rules adopted by the agencies, many of these permitted the use of the information for legal law enforcement purposes (Cagle, 2013, p. 1).

Use of information in criminal investigations and prosecutions

Documents procured by the ACLU proffered that the Federal Bureau of Investigation bought a small number of LPRs and sent to various field offices. The LPRs, brought from ELSAG North America, claims to have the capacity of being able to record approximately 1, 800 license plates a minute. The FBI proffered that the technology was only used in circumstances when the LPR is believed to help in furthering an investigation. A representative for the FBI stated that no " general data grab" was done of license plates on a random basis or storing the same in large data stores. With the aid of the Office of the Government Counsel (OGC), the organization developed guidelines in the use of the technology affecting privacy concerns (Pilkington, 2015, p. 1).

In Georgia, the readers can be utilized in any manner that the police or other law enforcement officials see fit. New Hampshire has banned the use of these readers within their jurisdiction; Maine has adopted a law that mandates the purging of the information from the system within a period of 21 days unless the information is being used as part of an ongoing law enforcement operation.

New Jersey has laws that stipulate that the information can only be kept for a period of five years. At the same time, California, Massachusetts, Michigan and Connecticut are contemplating on adopting laws that will curtail the use of these readers within their jurisdictions. For its part, the ACLU and its associates are requesting various state and local police agencies for information on the details that their own readers gather (Cook, 2012, p. 1).

Individuals who have access

Critical personal information gathered with the use of the LPR technology is distributed with other local jurisdictions and even possibly the Federal intelligence structure by way of a “ fusion centers.” These facilities were initially developed to provide a distribution and coordination center for anti-terrorism information across all levels of the law enforcement system. Though developed distinctly for another purpose, the scope of the objective of the structure has been significantly widened.

With the aid and “ encouragement” of the national government, the design of the facilities was expanded to include “ all crimes and all hazards.” The classes of data that the centers process have also widened to incorporate not only criminal information, but data coming from the public and private sector, and the stakeholders engaging the services of these agencies have come to include not only law enforcement agencies, but also entities from the private sectors, the military and other government agencies.

The operations as well as the philosophies guiding the running of the centers have raised serious concerns over privacy at a time when cutting edge technologies, strengthened government powers and near fanaticism in the conduct of the “ War on Terrorism” are amalgamating to place at risk the privacy of every American at a level never seen before. In addition, there are crucial questions on whether “ data fusion” is an effective tool in combatting extremism or a wise allocation for scarce government funding (ACLU, 2015, p. 1).

However, it must be noted that since no two centers are completely alike, it is a complex action to give sweeping statements regarding their actions. It is

clear that not all fusion facilities engage in inappropriate surveillance activities and not all centers generate civil liberties or privacy debates. However, there are those that are engaged in surveillance activities and an absence of legal safeguards that seeks to regulate their actions is dangerous.

The lack of legitimate legal boundaries on the operations of the fusion facilities not only poses a risk for traditional American norms, it also threatens to transform these entities into destructive and mismanaged parts of the bureaucracy similar to the national security and law enforcement structures prior to 9/11. Eventually, if the present approaches are not changed, these entities will not only waste tremendous amounts of public funds, these will be ineffective against any form of criminal activity (ACLU, 2015, p. 1).

Public safety concerns

The possibility of abusing the tenets of the program has been addressed by Federal statutes-the Drivers Privacy Protection Act- setting non-negotiable limits on the possibilities and the manner unnamed license palate date can be linked to data in the Department of Motor Vehicles (DMV) that is identity specific. Without access to the federally safeguarded database, it will be impossible for any person to connect a person with the data taken by the readers. The law at best is vague in terms of being able to connect the data with the identity of an actual individual (Vigilant, 2015, p. 1).

These technologies have the capacity to generate perpetual records of almost every motorist and track all the destinations one has been to; this

feature revolutionizes the effects of leaving one’s home in order to go about one’s private affairs, and opening up the possibilities for abuse. Monitoring the location of people comprises a large-scale intrusion of the government into the exercise of the right to privacy of all people; being able to track the movements of people comprises an invasion in that the policy will be able to give legal ambit to law enforcers to track the exact whereabouts of people, or those that the government wishes to target (ACLU, 2015, p. 1).

The technologies must solely be used to attain particularized law enforcement objectives and not as a mechanism as a tool for mass monitoring. At present, sloppy protections on the usage of the technology and the accessibility of the stored data by the Federal intelligence community generates significant problems regarding individual privacy. Actual safeguards formed through democratic debates can illuminate the issue regarding the use of the technology and the formulation of safeguards to prevent the abuse of the same (ACLU, 2015, p. 1).

It is but right to utilize these scanners to identify vehicles suspected in criminal activities; however, the technology must never be used to store information in data stores. The movements of people not on any criminal watch list must never be taken in activities where there is the possibility of abuse. Regrettably, ICE policy makers have developed these mass monitoring systems and have even pushed for their further application. This policy infringes on the long held practice that the government will not stalk its citizens unless the government has a legitimate reason to do so (Stanley, Stein, 2015, p. 1). Unless the government believes that all Americans are criminals, then it must address the concerns of its citizens, for real.

References

American Civil Liberties Union (2015) “ Automatic license plate readers” Retrieved July 15, 2015 from American Civil Liberties Union (2008) “ What’s wrong with fusion centers?” Retrieved July 15, 2015 from American Civil Liberties Union (2015) “ You are being tracked: how license plate readers are being used to record American’s movements.” Retrieved July 15, 2015 from Cagle, M (2013) “ Use of automated license plate readers expanding in Northern California, and data is shared with Feds” Retrieved July 15, 2015 from Cook, R (2012, November 30) Are automatic license plate readers a violation of privacy? Atlanta Journal Constitution

Herrera, V (2015) “ Are license plate scanners capturing too much?” Retrieved July 15, 2015 from Last Refuge (2015) “ DEA uses license plate readers to build data base for Federal, local authorities” Retrieved July 15, 2015 from Pilkington, E (2015, May 15) FBI had internal concerns over license plate readers, documents reveal. The Guardian

Sherfinski, D (2008, July 16) Feds seek to expand use of license tag readers in Va. Washington Examiner

Stanley, J., Stein, B. (2015) “ DHS wants contract for access to database of innocent driver’s locations.” Retrieved July 15, 205 from Vigilant Solutions (2015) “ Lawsuit challenges state of Utah ban on license plate readers as unconstitutional censorship of photography and violation of 1st Amendment” Retrieved 15 July 2015 from Watson, L (2014, April 18) Putting license plate readers to the constitutional test. Alexandria Times Alexandria Virginia