

Attachment #5

News Publications Concerning License Plate Recognition Systems and their Use

Washington Post, Forbes Magazine, Government Computer News

Forbes

HIGH-PERFORMANCE ANALYTICS
Decisions at the speed of right.
LEARN MORE ABOUT HIGH-PERFORMANCE ANALYTICS.

sas



Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

SECURITY | 8/21/2012 @ 2:29PM | 2,745 views

U.S. Customs Tracks Millions Of License Plates And Has Shared Data With Insurance Firms

Updated below with the date of the Department of Homeland Security documents.

It may come as little surprise that every time you cross the border, cameras record your license plate number and feed it into a database of driver locations. More disturbing, perhaps, is the fact that the government seems to share that automobile surveillance data with an unexpected third party: insurance companies.



A license plate reader camera mounted on a patrol car.

Documents obtained through a Freedom of Information Act request and released Tuesday by the Electronic Privacy Information Center (EPIC) catalogue just how pervasive automatic license plate readers have become at the Mexican and Canadian borders, with cameras placed in dozens of U.S. cities each capturing images of millions or tens of millions of plates a year. But the FOIA'd records (PDF [here](#)) also include memos outlining the sharing of that license plate data between the Department of Homeland Security's Customs and Border Protection, the Drug Enforcement Agency, and most significantly, the National Insurance Crime Bureau, an Illinois non-profit composed of hundreds of insurance firms including branches of Allstate, GEICO, Liberty, Nationwide, Progressive, and State Farm.

"This is warrantless collection of very private data, location data about where you've been and when," says Ginger McCall, an attorney with EPIC. "It's being shared with unknown organizations, not just in the government where there may be Privacy Act protections, but outside the government with third parties, possibly in contravention of the Privacy Act."

According to a ~~an undated~~ 2005 "memorandum of understanding" included in EPIC's document release, license-plate reader "information on vehicles departing from and arriving into the United States will be provided to the [National Insurance Crime Bureau or] NICB for the purpose of deterring the export of stolen vehicles, identifying vehicle theft patterns and trends...and returning vehicles to the rightful parties of interest." The data can also be used, according to the document, to identify so-called "owner-give-up" insurance fraud, in which a vehicle's owner fakes its theft by giving it to a friend and claiming it as stolen.

Preventing theft and fraud may seem like legitimate uses of that license plate data. But EPIC's McCall warns that once the data has found its way into the hands of a third party without public scrutiny, it may be far tougher to control how it's used. "Who can these third parties share their data with? What other ways might it be shared?" she asks. "You have to think about the ways this data slowly spreads out to third parties, and who then has access to it. It shouldn't be shared, and if it is, there should be more transparency about the details of who's doing the sharing, how it's used and how long the data is retained."

EPIC's documents, the first substantive response they've received to FOIA requests filed to a number of government agencies about the license plate readers starting more than a year ago, note that the license plate data is stored for two years, "unless

the data is moved to and maintained in a system that is governed by an alternate destruction schedule.”

I’ve put in a call to Customs and Border Protection’s public affairs office, but haven’t yet received a response from the agency. I’ll update this post when I do.

Automatic license plate reading cameras, mounted on utility poles, bridges and police patrol cars, have been coming under fire as they’ve been rolled out across the country. Last month the American Civil Liberties Union warned that the technology is quickly becoming “a warrantless tracking tool, enabling retroactive surveillance of millions of people,” and announced it’s sending requests for information to 38 police departments as well as the Departments of Justice, Homeland Security, and Transportation inquiring about the use of the technology.

Earlier this year, the New York Police Department was found to be using the license plate readers as part of an effort to surveil Muslim communities in Newark, New Jersey, without evidence that the targets had engaged in any prior criminal activity.

EPIC’s McCall points out that the use of the cameras may conflict with the Supreme Court’s January ruling in the U.S. v. Jones case, which stated that police can’t place GPS-enabled trackers on a car without a warrant. “The idea of that verdict was that the government shouldn’t be able to collect information wholesale about people’s location and movements,” says McCall. “There are very troubling privacy implications when information is collected and shared with third parties for purposes the public doesn’t know.”

See EPIC’s full release of documents below.



July 30, 2012

Kimberly Koopman, IPIOP Clerk
Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200

- [Download](#)
- [Share](#)
- [Embed](#)

• 1
of 20

This article is available online at:

<http://www.forbes.com/sites/andygreenberg/2012/08/21/documents-show-u-s-customs-tracking-millions-of-license-plates-and-sharing-data-with-insurance-firms/>



**U.S. Customs and
Border Protection**
DIS-2:OT:CTE:FD PH
2012F24299

July 30, 2012

Kimberly Koopman, IPIOP Clerk
Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009

Dear Ms. Koopman:

This is a partial response to your Freedom of Information Act (FOIA) request to U.S. Customs and Border Protection (CBP). You requested the following information:

1. All legal analyses, legal memoranda, final decisions, images, and related records regarding the national LPR initiative in its current or previous forms;
2. All documentation, including but not limited to guidelines, data retention policies, and training manuals, relating to the data collection process, usage, and storage of information gathered by the LPR initiative;
3. Any privacy impact assessments, privacy impact statements, and protocols performed, both past and present, for the DICE program and the LPR initiative;
4. Any memoranda of understanding between the DHS, DOJ, or any other federal, state, or local level government agencies, sub-agencies, or task forces in regard to the LPR initiative.

A search of CBP databases produced a total of 73 pages of records responsive to your request. CBP has determined that 18 pages of the records are partially released, pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)(C) and (b)(7)(E). The remaining 55 pages have been withheld in full pursuant to (b)(7)(E). Please note that these pages are in reference to parts two, three and four of your request.

Please also note that certain information such as Privacy Impact Assessments (PIA's) and System of Record Notices (SORNs) may be located online, either in the Federal Register or in CBP's online FOIA library, located at <http://foia.cbp.gov/>.

Please also note that we are still collecting records in response to part one of your request.

Exemption (b)(6) exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right privacy. *[The types of documents and/or information that we have withheld may consist of birth certificates, naturalization certificates, driver license, social security numbers, home addresses, dates of birth, or various other documents and/or information belonging to a third party that are considered personal.]* The privacy interests of the individuals in the records you have requested

outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption (b)(7)(C) protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate.

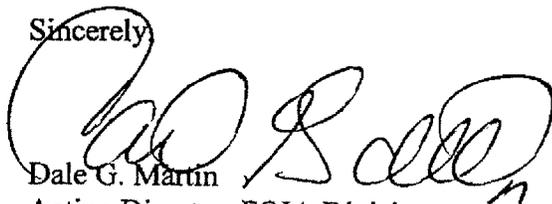
Exemption (b)(7)(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

You have a right to appeal our withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: FOIA Appeals, Policy and Litigation Branch, U.S. Customs and Border Protection, 799 Ninth Street, NW, 5th Floor, Washington, DC 20229-1179, following the procedures outlined in the DHS regulations at Title 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at ogis@nara.gov or call (877) 684-6448.

This office may be reached at (202) 325-0150. Please notate file number 2012F24299 on any future correspondence to CBP related to this request.

Sincerely



Dale G. Martin
Acting Director, FOIA Division
Office of International Trade

Enclosure(s)



**U.S. Customs and
Border Protection**

MAR 24 2010

MEMORANDUM FOR: See Distribution (B)(6), (B)(7)(C)
FROM: Executive Director (B)(6), (B)(7)(C)
Admissibility and Passenger Programs
SUBJECT: License Plate Reader (LPR) Directive (B)(7)(E)
Superseded by this Memorandum

The Western Hemisphere Travel Initiative (WHTI) has replaced all first generation License Plate Readers (LPR) with a new updated system for all inbound lanes. WHTI has also begun to replace the outbound LPRs that are at the end of their lifecycle. Effective upon receipt, this Memorandum supersedes LPR Directive (B)(7)(E). The below listed bullets will reflect current requirements for LPRs:

- LPRs are required to be functioning properly and capturing plate images at all times.
- The Port Director is responsible for ensuring LPRs are functioning properly at a port.
- When an LPR is not functioning properly the officer is required to report the problem to the shift supervisor. The supervisor will follow local policy to assure that a work ticket is opened immediately.
- When an LPR unit is not functioning, the license plates of all inbound vehicles must be queried manually by the officer assigned to the primary booth. Officers should monitor LPR queries (B)(7)(E)
- Only the Field Technical Officers (FTO) are authorized, as necessary, to clean the LPR equipment. Under no circumstances should any LPR equipment be cleaned, repaired or tampered with by port staff.
- The OFO LPR Program Manager will establish a national review program. The review program will also look for error patterns and report these to the appropriate level.
- Ports and Field Offices are no longer required to perform Self Inspection Program (SIP) for verifying quarterly accuracy of LPR plate images. The current, next generation LPRs are automated and monitored nationally for accuracy.

~~For Official Use Only
Law Enforcement Sensitive~~

LPR requirements will be incorporated into the next version of CBP Directive Number (B)(7)(E)

(B)(7)(E)

If you have any questions or concerns, please have a member of your staff contact (B)(6), (B)(7)(C) (B)(6), (B)(7)(C) Director, WHTI, or (B)(6), (B)(7)(C) Program Manager at (B)(6), (B)(7)(C)

Distribution:

Director, Field Operations, Buffalo
Director, Field Operations, Detroit
Director, Field Operations, El Paso
Director, Field Operations, Laredo
Director, Field Operations, San Diego
Director, Field Operations, Seattle
Director, Field Operations, Tucson
Director, Field Operations Academy

~~For Official Use Only
Law Enforcement Sensitive~~

MEMORANDUM OF UNDERSTANDING
between the
U.S. DEPARTMENT OF JUSTICE,
DRUG ENFORCEMENT ADMINISTRATION
and
U.S. DEPARTMENT OF HOMELAND SECURITY,
U.S. CUSTOMS AND BORDER PROTECTION
regarding
SHARING OF LICENSE PLATE READER DATA

1. PARTIES

The Parties to this Memorandum of Understanding (MOU) are the U.S. Department of Justice (DOJ), Drug Enforcement Administration (DEA), and the U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), collectively "the Parties."

2. PURPOSE

The purpose of this MOU is to support the missions of DEA and DHS by establishing the terms and conditions for the sharing of the Parties' license plate reader (LPR) data and to authorize further dissemination of the Parties' license plate reader data.

3. DEFINITIONS

3.1. LPR

"License plate reader" or "LPR" data means the license plate number, state of origin, and digital images collected by either Party after the effective date of this MOU relating to vehicles transiting through ports of entry, checkpoints, or other locations where license plate readers are operated by the parties, and includes the date, time, and location of collection.

4. AUTHORITIES

4.1. DHS

DHS is authorized to enter into this MOU pursuant to the Homeland Security Act of 2002, Pub. L. No. 107-296 § 101, 102, and 202 as amended, which vests the Secretary of DHS and his or her designee with the authority to enter into agreements with other Executive Agencies to, in pertinent part, ensure that intelligence or other information relating to terrorism and narcotics trafficking that DHS has access to is appropriately shared with any other element of the Federal Government with responsibility for analyzing terrorist and narcotics threat information.

Furthermore, DHS has determined that DOJ access to LPR data, as set forth in the MOU, is appropriate pursuant to authority granted under the provisions of the Comprehensive Drug

Abuse Prevention and Control Act of 1970, as amended, 21 U.S.C. § 801 *et seq.*, in addition to Executive Orders and other guidance applicable to all Federal agencies.

4.2. *DEA*

DEA is authorized to enter into this MOU pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, 21 U.S.C. § 801 *et seq.* The specific authority for DEA to enter into cooperative agreements for the exchange of information between governmental officials concerning the use and abuse of controlled substances is set forth under 21 U.S.C § 873.

5. *RESPONSIBILITIES*

5.1. *Data sharing*

CBP will provide DEA with LPR data collected by CBP and DEA will provide CBP with LPR data collected by DEA at regular intervals and in a manner specified in a separate, service-level agreement between the Parties.

5.2. *Use of LPR data*

Each Party's use of data shared, pursuant to this MOU, will be in accordance with the purposes stated in this MOU and any applicable laws and regulations.

DHS and DOJ are authorized to incorporate and disseminate LPR data received from each other into documents such as reports, affidavits, legal process, case files, and analytical products.

6. *CONFIDENTIALITY*

6.1. *Access*

The Parties will limit access to any LPR data received, pursuant to this MOU, to only those authorized personnel who have a need to know in the performance of their official duties.

6.2. *Dissemination*

Except as otherwise provided below, data received pursuant to this MOU will not be disseminated outside of DHS or DOJ without the express prior-written consent of the providing Party, unless dissemination is required by U.S. law or regulation.

The Parties agree that any LPR data provided by the other Party, or analytical product containing such data, will be de-conflicted jointly by the staff of both Parties (B)(7)(E) (B)(7)(E) at the (B)(7)(E) or any successor entity designated by both parties, before any operational action is taken on the basis of the data or product.

The dissemination of LPR data received under this MOU to Federal, state, and local law enforcement and prosecutors in the performance of their official duties is permitted under this MOU where otherwise in conformance with applicable law. Non-Party recipients of LPR data disseminated under this MOU will be instructed to coordinate and de-conflict any resulting operational activity through (B)(7)(E)

Furthermore, the dissemination of LPR data to intelligence, operations, and fusion centers, including the (B)(7)(E) is permitted under this MOU where otherwise in conformance with applicable law.

The dissemination set forth above will be expressly conditioned upon the receiving authority's compliance with the terms of this MOU and regarding the treatment and handling of the LPR data.

6.3 Third Party Requests

When a Party receives a request, including requests under the Freedom of Information Act or the Privacy Act, from a third party not otherwise covered by the MOU for data received under this MOU, that Party will ensure that it does not adjudicate the request on behalf of the providing Party.

Upon receiving such requests, the receiving Party will consult with the Party that provided the LPR data of how to respond to the request and, if appropriate, will refer the request to the providing Party for response.

6.4 Data Markings

All LPR data shared pursuant to this MOU must contain markings identifying the providing agency and the nature of the data. Based on these markings and the nature of the data provided, the receiving agency will be required to apply appropriate handling and safeguarding measures as required by law and applicable policy.

7. DATA SECURITY, RETENTION, AND INTEGRITY

7.1. Safeguards

The Parties agree to maintain administrative, technical, and physical safeguards appropriate to the sensitivity of, and designed to appropriately protect, the LPR data shared under this Agreement against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification, storage, or deletion in accordance with the Federal Information Security Management Act (FISMA) and any applicable Privacy Act system of records notices. These safeguards must include audit capabilities that identify the LPR data the Parties disseminated pursuant to section 6.2 of this MOU, and a point of contact within the entity receiving the LPR data to provide audit information.

7.2. *Retention*

The Parties will destroy LPR data received under this MOU two years after receipt, unless the data is moved to and maintained in a system that is governed by an alternate destruction schedule. In the event that LPR data is maintained in a Privacy Act system or systems of records, the data shall be maintained, shared, and used in accordance with the applicable Privacy Act System of Records Notice(s).

7.3. *Unauthorized Activity Reporting*

Where there has been or may have been unauthorized access, disclosure, copying, use, modification, storage, or deletion of data received under this MOU, the Party discovering the unauthorized activity will promptly report to, and consult with, the other Party through the points of contact identified herein, in accordance with each Party's incident reporting policies.

8. *COSTS*

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

9. *POINTS OF CONTACT*

The following individuals, and their successors, shall be the point of contact for each Party regarding the implementation, amendment or termination of this MOU:

(B)(6), (B)(7)(C) Director, Office of Field Operations, CBP

(B)(6), (B)(7)(C) Associate Chief Enforcement, Office of Border Patrol, CBP

(B)(6), (B)(7)(C) Deputy Assistant Administrator, DEA

(B)(6), (B)(7)(C) Chief of Financial Operations, DEA

10. *SEVERABILITY*

Nothing in this MOU is intended to conflict with current law or regulation or the policies of DHS and DOJ. If a term of this MOU is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

11. EFFECT ON OTHER AUTHORITIES

Nothing in this MOU is intended to restrict the authority of either Party to act as provided by law, statute, or regulation, or to restrict either Party from administering or enforcing any laws within its authority or jurisdiction.

12. EFFECTIVE DATE

The terms of this MOU will become effective upon signature by both Parties.

13. MODIFICATION

This MOU may be modified in writing upon the mutual-written consent of the Parties.

14. TERMINATION

Either Party may terminate this MOU upon thirty (30) days written notice to the other Party. In the event of termination, all provisions regarding the protection of LPR data received under this MOU, including data privacy, retention, and confidentiality, remain in effect as long as either Party remains in possession of any LPR data received under this MOU from the other Party.

15. NO PRIVATE RIGHTS CREATED

This MOU does not create any right or benefit, substantive or procedural, enforceable in law or in equity, against the United States, its departments, agencies, or other entities, its officers, employees, or any other person.

(B)(6), (B)(7)(C)

Alan D. Bersin
Commissioner
U.S. Customs and Border Protection
U.S. Department of Homeland Security

(B)(6), (B)(7)(C)

Michele Leonhart /
Acting Administrator
U.S. Drug Enforcement Administration
U.S. Department of Justice

**Western Hemisphere Travel Initiative
Deployment Schedule for Top 13 High Volume POEs**

Scope	Lanes	% complete	completed lanes	387	current lanes	0	Total lanes
expanded	388	99.7%	completed crossings	62	upcoming lanes	0	lanes
original	354	109.3%	completed ports	42	remaining lanes	1	388

Port / Facility	DCL Lanes	FY06 PAX			Construction				Installation			# of Lanes
		Crossing Volume	% of Crossing Volume	Cumulative Crossing %	VPC Go Live	Begin	End	Begin	End	Go Live		
Blaine, WA		5,165,281	2.11%	2.11%								
Pacific Highway	1				12-Feb-08	9-Jun-08	8-Aug-08	8-Sep-08	26-Sep-08	27-Sep-08	5	
Peace Arch (A)	1				29-Sep-08	23-Jun-08	5-Aug-08	15-Sep-08	26-Sep-08	27-Sep-08	4	
Peace Arch (B)						11-Nov-10	12-Nov-10	15-Nov-10	20-Nov-10	21-Nov-10	3	
Peace Arch (C)								17-Jan-11	28-Jan-11	29-Jan-11	1	
Nogales, AZ		8,650,524	3.54%	5.65%								
Nogales, AZ West	1				12-Feb-08	23-Jun-08	23-Jun-08	8-Sep-08	19-Sep-08	20-Sep-08	4	
Nogales, AZ East					14-Feb-08	23-Jun-08	5-Aug-08	6-Oct-08	16-Oct-08	17-Oct-08	8	
Buffalo, NY		13,535,244	5.54%	11.19%								
Lewiston	1				2-Jun-08	14-Jul-08	18-Jul-08	20-Oct-08	5-Nov-08	6-Nov-08	7	
Peace Bridge	2				2-Jun-08	21-Jul-08	6-Aug-08	20-Oct-08	21-Nov-08	22-Nov-08	16	
Rainbow Bridge (A)	1				2-Jun-08	8-Oct-08	24-Oct-08	20-Oct-08	12-Nov-08	13-Nov-08	14	
Rainbow Bridge (B)					2-Jun-08			23-Jun-09	26-Jun-09	27-Jun-09	3	
Whitpool Bridge	2				2-Jun-08	14-Jul-08	18-Jul-08	5-Nov-08	6-Nov-08	7-Nov-08	2	
Detroit, MI		10,136,290	4.15%	15.34%								
Ambassador Bridge	2				9-Jun-08	14-Jul-08	26-Jul-08	20-Oct-08	18-Nov-08	19-Nov-08	19	
Windsor Tunnel	2				9-Jun-08	21-Jul-08	5-Aug-08	20-Oct-08	12-Nov-08	13-Nov-08	9	
Brownsville, TX		14,171,099	5.80%	21.14%								
B&M Bridge					14-Aug-08	6-Aug-08	8-Aug-08	1-Dec-08	11-Dec-08	12-Dec-08	4	
Gateway Bridge					14-Aug-08	31-Jul-08	5-Aug-08	1-Dec-08	15-Dec-08	16-Dec-08	5	
Los Indios					13-Aug-08	25-Jul-08	5-Aug-08	1-Dec-08	11-Dec-08	12-Dec-08	4	
Veteran's Bridge	1				13-Aug-08	11-Aug-08	12-Aug-08	1-Dec-08	12-Dec-08	13-Dec-08	4	
Olay Mesa, CA	1	11,447,926	4.68%	25.82%	29-Sep-08	16-Sep-08	25-Sep-08	1-Dec-08	16-Dec-08	17-Dec-08	13	
Calixico East, CA		7,801,534	3.19%	29.01%	16-Jun-08	22-Aug-08	29-Aug-08	1-Dec-08	16-Dec-08	17-Dec-08	8	
San Ysidro, CA	4	31,741,363	12.99%	42.00%	8-Sep-08	4-Aug-08	8-Aug-08	5-Jan-09	13-Feb-09	14-Feb-09	24	
Calixico, CA	1	11,262,530	4.61%	46.61%	16-Jun-08	15-Sep-08	30-Jan-09	19-Jan-09	4-Feb-09	5-Feb-09	10	
El Paso, TX		28,608,705	11.71%	58.32%								
Stanton Street	3				7-Jul-08	22-Sep-08	9-Oct-08	5-Jan-09	12-Jan-09	13-Jan-09	3	
BOTA (Bridge of the Americas)					7-Jul-08	2-Sep-08	26-Sep-08	5-Jan-08	6-Feb-09	7-Feb-09	14	
Paso del Norte					7-Jul-08	18-Aug-08	29-Aug-08	5-Jan-09	5-Feb-09	6-Feb-09	12	
Ysleta	2				7-Jul-08	30-Jul-08	14-Aug-08	5-Jan-09	22-Jan-09	23-Jan-09	12	
Laredo, TX		14,107,583	5.77%	64.09%								
Columbia					25-Aug-08	1-Aug-08	6-Aug-08	19-Jan-09	26-Jan-09	27-Jan-09	4	
Convent-Bridge 1	2				25-Aug-08	4-Aug-08	8-Aug-08	2-Feb-09	12-Feb-09	13-Feb-09	4	
Lincoln-Juarez-Bridge 2					25-Aug-08	18-Aug-08	22-Aug-08	9-Feb-09	2-Mar-09	3-Mar-09	12	
Hidalgo, TX		12,953,555	5.30%	69.39%								
Hidalgo	1				18-Aug-08	19-Aug-08	3-Sep-08	9-Feb-09	5-Mar-09	6-Mar-09	13	
Pharr					18-Aug-08	15-Aug-08	27-Aug-08	2-Feb-09	13-Feb-09	14-Feb-09	6	
Eagle Pass, TX		8,517,673	3.49%	72.87%								
Eagle Pass Bridge 1					16-Mar-09	11-Aug-08	15-Aug-08	9-Mar-09	18-Mar-09	19-Mar-09	5	
Eagle Pass Bridge 2					16-Mar-09	11-Aug-08	15-Aug-08	16-Feb-09	2-Mar-09	3-Mar-09	6	

28

page total/ 259

Western Hemisphere Travel Initiative
Deployment Schedule for Remaining High Volume POEs

completed lanes current lanes upcoming lanes remaining lanes

Port / Facility	DCL Lanes	Crossing Volume	FY06 PAX		VPC Go Live	Construction		Installation		# of Lanes
			% of Crossing Volume	Cumulative Crossing %		Begin	End	Begin	End	
Top 13	28	178,099,307	72.87%	73.43%						259
Andrade, CA (A)		1,354,529	0.55%	73.43%	16-Jun-08	12-Sep-08	15-Sep-08	12-May-09	14-May-09	15-May-09
Andrade, CA (B)					16-Jun-08	12-Sep-08	15-Sep-08	Spring 2012	8-Mar-12	9-Mar-12
Andrade, CA (C)					16-Jun-08	12-Sep-08	15-Sep-08	TBD	TBD	TBD
San Luis, AZ		5,503,418	2.25%	75.68%						
San Luis, AZ (A)					21-Jul-08	8-Sep-08	12-Sep-08	2-Mar-09	17-Mar-09	18-Mar-09
San Luis, AZ (B)					4-Dec-10	7-Nov-10	19-Nov-10	29-Nov-10	3-Dec-10	4-Dec-10
Columbus, NM		1,123,601	0.48%	76.14%	18-Sep-08	2-Sep-08	5-Sep-08	2-Feb-09	5-Feb-09	6-Feb-09
Douglas, AZ		4,406,880	1.80%	77.94%	29-Sep-08	2-Sep-08	4-Sep-08	23-Feb-09	4-Mar-09	5-Mar-09
Tecate, CA		1,906,693	0.78%	78.72%	14-Jun-08	2-Sep-08	12-Sep-08	17-Nov-08	21-Nov-08	22-Nov-08
Rio Grande City, TX		2,216,312	0.91%	79.63%	18-Aug-08	3-Nov-08	14-Nov-08	16-Feb-09	21-Feb-09	22-Feb-09
Fabens, TX		1,242,617	0.51%	80.14%						
Fabens, TX					15-Sep-08	4-Aug-08	14-Aug-08	17-Nov-08	21-Nov-08	22-Nov-08
Fort Hancock, TX					15-Sep-08	4-Aug-08	8-Aug-08	17-Nov-08	20-Nov-08	21-Nov-08
Presidio, TX		1,630,347	0.67%	80.81%	9-Dec-08	25-Aug-08	9-Sep-08	12-May-09	19-May-09	20-May-09
Roma, TX		2,805,783	1.15%	81.95%	18-Aug-08	3-Nov-08	14-Nov-08	16-Mar-09	24-Mar-09	25-Mar-09
Lukeville, AZ		1,236,121	0.51%	82.46%	21-Jul-08	3-Nov-08	7-Nov-08	14-Apr-09	17-Apr-09	18-Apr-09
Progreso, TX		2,413,725	0.99%	83.45%	13-Aug-08	1-Dec-08	11-Dec-08	2-Mar-09	11-Mar-09	12-Mar-09
Del Rio, TX		4,032,369	1.65%	85.10%	11-May-09	17-Nov-08	22-Nov-08	23-Mar-09	3-Apr-09	4-Apr-09
Sumas, WA		1,241,057	0.51%	85.60%	22-Sep-08	30-Oct-08	7-Nov-08	18-Mar-09	24-Mar-09	25-Mar-09
Point Roberts, WA	1	1,865,326	0.76%	86.37%	22-Sep-08	27-Oct-08	7-Nov-08	9-Mar-09	12-Mar-09	13-Mar-09
Lynden, WA		983,157	0.40%	86.77%	22-Sep-08	30-Oct-08	7-Nov-08	16-Mar-09	23-Mar-09	24-Mar-09
FLETC			0.00%	86.77%	24-Apr-09	9-Feb-09	10-Feb-09	23-Mar-09	31-Mar-09	1-Apr-09
Messena, NY		1,908,107	0.78%	87.55%	30-Jun-08	15-Sep-08	19-Sep-08	27-Apr-09	29-May-09	16-Jun-09
Highgate Springs/Alburt, VT		889,844	0.36%	87.91%						
Alburt, VT					29-Jul-08	14-Apr-09	16-Apr-09	27-Apr-09	29-Apr-09	30-Apr-09
Highgate Springs, VT					28-Jul-08	14-Apr-09	22-Apr-09	14-Apr-09	22-Apr-09	23-Apr-09
Champlain-Rouses Point, NY		2,873,208	1.18%	89.08%						
Champlain	1				23-Jun-08	22-Sep-08	26-Sep-08	23-Mar-09	3-Apr-09	4-Apr-09
Rouses Point					23-Jun-08	19-Apr-09	23-Apr-09	4-May-09	8-May-09	9-May-09
Port Huron, MI	1	4,121,872	1.69%	90.77%	8-Sep-08	15-Sep-08	19-Sep-08	23-Mar-09	3-Apr-09	4-Apr-09
Sault Sainte Marie, MI	1	1,670,526	0.68%	91.45%	11-Sep-08	15-Sep-08	19-Sep-08	5-May-09	9-May-09	10-May-09
Houlton, ME (A)	1	713,064	0.29%	91.74%	4-Aug-08	14-Apr-09	18-Apr-09	27-Apr-09	3-May-09	3-May-09
Houlton, ME (B)					4-Aug-08	June 2012	June 2012	5-Jun-12	5-Jun-12	8-Jun-12
Pembina, ND	1	777,651	0.32%	92.06%	22-Sep-08	8-Oct-08	10-Oct-08	27-May-09	5-Jun-09	6-Jun-09
Derry Line, VT		1,274,164	0.52%	92.58%						
Derry Line, VT L91					28-Jul-08	13-Oct-08	25-Oct-08	31-Mar-09	7-Apr-09	8-Apr-09
Derry Line, VT Rie 5					28-Jul-08	22-Oct-08	26-Oct-08	31-Mar-09	6-Apr-09	7-Apr-09
Calais, ME		2,585,775	1.06%	93.64%	4-Aug-08	13-Oct-08	26-Sep-08	14-Apr-09	17-Apr-09	18-Apr-09
Medawaska, ME		1,116,033	0.46%	94.10%	4-Aug-08	26-Apr-09	28-Apr-09	5-May-09	7-May-09	8-May-09
International Falls/Rainier, MN	1	1,175,380	0.48%	94.68%	26-Sep-08	20-Oct-08	30-Oct-08	20-Apr-09	24-Apr-09	25-Apr-09
Sweetgrass, MT	1	869,553	0.36%	94.94%	22-Sep-08	14-Apr-09	16-Apr-09	16-Apr-09	21-Apr-09	22-Apr-09
Alexandria Bay, NY	1	1,566,372	0.64%	95.58%	30-Jun-08	14-Apr-09	24-Apr-09	20-Apr-09	6-May-09	7-May-09
	38									388

**MEMORANDUM OF UNDERSTANDING
BETWEEN
U.S. CUSTOMS AND BORDER PROTECTION
AND
THE NATIONAL INSURANCE CRIME BUREAU**

The parties to this Memorandum of Understanding (MOU) are U.S. Customs and Border Protection (CBP), a bureau within the Department of Homeland Security (DHS), and the National Insurance Crime Bureau (NICB), an Illinois not-for-profit organization.

The objective of this MOU is to set forth the parameters of the sharing of License Plate Reader (LPR) information, regarding vehicles departing from and arriving into the United States, between the parties.

The purpose of furnishing LPR information is to verify that vehicles departing from and arriving into the United States are not stolen vehicles. NICB has access to unique information regarding stolen vehicles, as well as the means of exchanging information regarding stolen vehicles with member insurance company Special Investigative Units and Federal and State law enforcement authorities.

The purpose of this MOU is to establish the parameters under which the NICB may use LPR information received from CBP. LPR information on vehicles departing from and arriving into the United States will be provided to the NICB for the purpose of deterring the export of stolen vehicles, identifying vehicle theft patterns and trends, identifying insurance fraud "owner-give-ups," and returning vehicles to the rightful parties of interest.

NICB and CBP are entering into this MOU on the authority provided in 19 U.S.C. § 1627a. Pursuant to 19 U.S.C. § 1627a(d), "CBP officers may cooperate and exchange information concerning motor vehicles ... either before exportation or after exportation, with such Federal, State, local and foreign law enforcement or governmental authorities, and with such organizations engaged in theft prevention activities, as may be designated by the Secretary."

By signature below, the President and Chief Executive Officer from NICB affirms, represents, and certifies that the Special Investigative Unit of each of the member insurance companies in the attached listing provided by NICB is an organization related to NICB that is engaged in theft prevention activity and is therefore an appropriate recipient of LPR information. NICB shall notify CBP immediately of any change in the theft prevention status of any company listed in the attachment hereto. Any entity no longer engaged in theft prevention activity shall be stricken immediately from the list, and no entity may be added to the list absent the approval of CBP.

By signature below, the Commissioner of CBP hereby finds, in recognition of and contingent upon a continuing certification from NICB, that the Special Investigative Unit of each of the member insurance companies in the attached listing provided by NICB is an organization engaged in theft prevention activity and therefore an appropriate recipient of LPR information.

WHEREAS, NICB and CBP desire that LPR information shall continue to be made available to NICB.

THEREFORE, NICB and CBP understand and hereby agree to the following:

I. CBP Agrees To:

1. Make available to NICB electronic LPR information on vehicles leaving or entering the United States.
2. Designate a working-level CBP systems representative to facilitate communications and interactions between CBP and NICB pursuant to this MOU.

II. NICB Agrees To:

1. Collect LPR information provided by CBP and load the LPR information into a database approved by CBP.
 2. Procure the equipment, software, and programming resources necessary to develop the capability to utilize, refine, and organize the information provided by CBP.
 3. Provide CBP with electronic access to the refined and organized LPR information, via a reasonable electronic system agreed upon by NICB and CBP.
 4. Notify CBP of any changes planned or being considered that would affect this MOU.
 5. Designate a working-level NICB systems representative to facilitate communications and interactions between CBP and the NICB.
 6. Restrict the dissemination of LPR information, on a need-to-know basis, to:
(a) authorized NICB agents and other employees of the NICB, (b) law enforcement officials in need of certain LPR records in furtherance of stolen vehicle investigations, and (c) Special Investigative Units of NICB member insurance companies listed in the attachment hereto that have been designated by CBP as organizations engaged in theft prevention activity.
-

7. NICB may not use the information obtained from CBP for commercial purposes or sell the information obtained from CBP to any third party.

III. NICB's Outsourcing of Data Operations with CBP Prior Written Approval

1. NICB may outsource data entry, database and telecommunications maintenance, and operation functions relating to the LPR database(s) to a data processing service (DPS), subject to the requirements of this MOU. If NICB desires to outsource the data processing operations, it must present to CBP the outsourcing agreement for written approval. The outsourcing agreement must expressly set forth the terms and conditions of the outsourcing. The outsourcing agreement must incorporate provisions to: maintain the highest degree of confidentiality of the information provided by CBP to NICB and prohibit dissemination of the data by DPS; place limitations on the access to the data by DPS personnel; identify the level of service to be provided; and assure the security of CBP data, as well as security of DPS premises. The furnishing of information by NICB to DPS is subject to the same strict confidentiality provisions to which NICB is bound. DPS must acknowledge that the information is subject to CBP's confidentiality and use restrictions and must agree to abide by such restrictions.

2. DPS may not access, modify, or use LPR information, or any other transactions or data generated or maintained as a result of NICB's relationship with CBP, in any manner not expressly approved by NICB, who in turn, must consult and obtain approval from CBP, or in any manner not expressly provided for elsewhere in this MOU. DPS shall return immediately all LPR information to CBP or NICB upon the request of either CBP or NICB, or at the termination of the DPS contract with NICB, whichever is sooner. DPS may not sell or otherwise distribute LPR information.

IV. Security Violations and Right to Suspend Services

1. NICB will notify CBP immediately, in writing, of any and all reported or suspected use or dissemination of LPR information that is violative of law or the terms of this MOU, or is otherwise unauthorized. NICB will require that any recipient of LPR information from NICB immediately report misuse of LPR information to NICB who will then report the misuse to CBP. CBP reserves the right to investigate or decline to investigate any report of unauthorized use or dissemination, and NICB and any DPS or other holder of LPR information shall grant full system and property access to CBP or DHS officers investigating an unauthorized use or dissemination of LPR information.

2. The services detailed within this MOU may be immediately suspended by CBP for unauthorized or improper use of the LPR information or any other cause, as determined by CBP. Any recipient of LPR information, including the

NICB and any DPS, shall immediately return all LPR information in its custody to CBP upon CBP suspension of this MOU and CBP demand for the return of LPR information. LPR information access may be reinstated at the discretion of CBP only after satisfactory assurances have been provided to CBP by the NICB.

V. Confidentiality

1. The information described in this MOU is transferred to NICB from CBP with the understanding that NICB is aware of and will comport its operations with the Computer Security Act of 1987; the Privacy Act, and Office of Personnel Management regulations concerning information security that are in effect at the time of transfer.
 2. NICB understands and acknowledges that LPR information is highly sensitive commercial, financial, and proprietary information; may only be reviewed by authorized NICB personnel or other entities pursuant to this MOU on a need-to-know basis; and must be kept secure. NICB agrees that LPR information obtained will be used only for the purposes of deterring the export of stolen vehicles, recovering stolen vehicles, and repatriating exported stolen vehicles.
 3. CBP considers the LPR information provided to NICB to be confidential commercial information, exempt from disclosure pursuant to the Freedom of Information Act (FOIA) and/or prohibited from disclosure by the Trade Secrets Act. As such, no information may be released without CBP express written permission as set forth in this MOU. NICB agrees that any outside request for LPR information in its custody or in the custody of an LPR data recipient or DPS will be referred to CBP for any response.
 4. It is recognized that a CBP-approved DPS to whom the NICB outsources data entry and/or data processing operations has responsibilities under the confidentiality agreement with NICB. Consequently, NICB may provide DPS with the information obtained from CBP. This information is provided to DPS with the restrictions that such data shall be reviewed only by authorized DPS personnel necessary to process the data, shall be kept secure, and shall not be passed on to third parties.
 5. NICB is responsible for any inappropriate disclosure of confidential information by NICB or DPS personnel or any other recipient of LPR information from NICB. In the event of any unauthorized release (a release not authorized by CBP or otherwise in violation of law or this MOU) of information, NICB will intercede on CBP's behalf and indemnify and assume responsibility for any and all expenses, costs, or liabilities arising from the unauthorized release. This clause will not limit NICB's ability to attribute damages to a DPS or other recipient within the provisions of their contractual obligation to NICB. Such unauthorized disclosure may result in denial of future access to information and abrogation of any implicated agreement.
-

VI. It is Mutually Understood and Agreed that:

1. The above provisions will be exercised to the extent authorized by law; DHS and CBP directives, statutes, policies, and regulations; and NICB bylaws and policies; and consistent with the respective parties' missions.
2. Nothing in this MOU shall obligate either CBP or NICB to obligate or transfer funds. Any specific work projects or activities that contemplate or involve the transfer of funds, services, or property among the various offices of CBP and NICB will require execution of separate agreements and be contingent upon the availability of appropriated funds. Such activities must be authorized by appropriate statutory authority, and this MOU does not provide such authority. Negotiation, execution, and administration of each such agreement must comply with all applicable statutes and regulations.
3. This MOU is a formal expression of the purpose and intent of both parties concerned. This MOU does not confer, grant, or authorize any rights, privileges, or obligations on any party other than the two undersigned parties to this MOU.
4. NICB acknowledges that CBP, at its sole and unreviewable discretion, may restrict or preclude the disclosure of information to NICB or any DPS or other recipient. This MOU is not intended to create, and does not create, any right, benefit, or trust responsibility, substantive or procedural, enforceable at law or equity, by a party against the United States, its agencies, its officers, or any person.
5. This MOU shall become effective upon the date of final signature and is intended to be in force until terminated by CBP pursuant to Article IV, or by the NICB upon 90 days written notice, or amended by mutual agreement of the undersigned. Such termination notices shall be forwarded by registered mail, postage prepaid, to the following addresses, respectively:

U.S. Customs and Border Protection
Office of Field Operations
1300 Pennsylvania Avenue NW
Ronald Reagan Building - Fifth Floor
Washington, DC 20229

President
National Insurance Crime Bureau
10330 South Roberts Road
Palos Hills, Illinois 60465

The undersigned parties, effective upon the date of last signature, hereby enter into this Memorandum of Understanding.

(B)(6), (B)(7)(C)

Robert C. Bonner 11-4-05 date
Commissioner
U.S. Customs and Border Protection

(B)(6), (B)(7)(C)

(B)(6), (B)(7)(C) 11/17/05 date
President and Chief Executive Officer
National Insurance Crime Bureau

Fixed and Mobile LPR units deployed outbound as of:

6/20/2012

Tier 2: (Note: Tier 2 solution consists of fixed in lane or gantry mounted LPRs

(B)(7)(E)

- San Luis construction was completed 6/12/2012. Fixed LPR installation was completed 6/15/2012. (B)(7)(E) were deployed 3/7/2012. Training for the fixed LPR and (B)(7)(E) configuration was provided in June 14-15.
- Douglas construction was completed 6/19/2012. Fixed LPR installation is scheduled for completion 6/22/2012. (B)(7)(E) were deployed to Douglas 2/8/2011. Training for the fixed LPR and (B)(7)(E) configuration will be provided in June 21-22.
- Developing 95% designs for Progreso, Rio Grande City and Calexico East – review conducted 6/20/2012

Tier 3:

- The Tier 3 deployments for all intents and purposes are complete. Antelope Wells – to be implemented coincident with the inbound deployment. Santa Teresa – to be implemented following relocation of the (B)(7)(E) Los Ebanos was removed from the schedule because of flood damage. There are currently no plans to add Los Ebanos back in to the schedule.

(B)(7)(E) Users Group:

- The (B)(7)(E) Users Group meeting was held June 4, 2012. The next meeting is scheduled for July 10, 2012.

MC75A Release 4:

- The upcoming (B)(7)(E) will be pushed to the field June 21, 2012. Release functionality will be pilot tested at Veterans and Gateway before it is pushed to all locations. Once it is confirmed that there are no issues with the release, the decision to move forward will be passed to the field during a conference call on June 21, 2012. It is expected that all locations will be actively processing vehicles and travelers with the new release before COB. The release will contain several user requested enhancements. A key new functionality is the device will no longer be tied to a specific port. Officers will be able to use the device at any site and it will automatically adjust to capture site specific crossing data.

Schedule: The schedule for the remaining locations is as follows:

- Douglas, Tier 2 Training 6/21-6/22/2012
- San Teresa, Tier 3 (2 units) TBD
- Antelope Wells, Tier 3 (1 unit) TBD

Completed Locations:

Tier 2 Upgrades have been successfully completed at:

5/18/2012 Eagle Pass 1

4/27/2012 Eagle Pass 2

6/15/2012 San Luis

(B)(7)(E) technology has been successfully deployed to:

4/20/2012 Columbus, Tier 3 (2 units)
4/17/2012 Presidio, Tier 3 (2 units)
4/4/2012 Ft Hancock, Tier 3 (1 unit)
4/3/2012 Fabens, Tier 3 (1 unit)
3/29/2012 Mariposa, Tier 3 (3 units)
3/29/2012 Columbia, Tier 3 (6 units)
3/29/2012 Eagle Pass 2, Tier 3 (2 units)
3/28/2012 Eagle Pass 1, Tier 3 (3 units)
3/27/2012 Naco, Tier 3 (1 unit)
3/27/2012 Convent, Tier 3 (4 units)
3/23/2012 Otay Mesa, Tier 3 (2 units)
3/23/2012 Tecate, Tier 3 (2 units)
3/20/2012 San Ysidro, Tier 3 (6 units)
3/15/2012 Falcon Dam, Tier 3 (1 unit)
3/14/2012 Roma, Tier 3 (2 units)
3/13/2012 Sasabe, Tier 3 (1 unit)
3/13/2012 Rio Grande City, Tier 3 (2 units)
3/8/2012 Lukeville, Tier 3 (2 units)
3/8/2012 Calexico West, Tier 3 (3 units)
3/7/2012 Calexico East, Tier 3 (2 units)
3/7/2012 San Luis, Tier 3 (2 units)
3/1/2012 Andrade, Tier 3 (1 unit)
2/27/2012 Progreso, Tier 3 (2 units)
2/28/2012 Donna, Tier 3 (2 units)
2/20/2012 Gateway, Tier 3 (3 units)
2/21/2012 B&M, Tier 3 (3 units)
2/22/2012 Los Indios, Tier 3, (2 units)
12/13/2011 Del Rio, Tier 2 (4 units)
12/13/2011 Amistad Dam, Tier 3 (1 unit)
12/8/2011 Ysleta, Tier 3 (7 units)
12/6/2011 BOTA, Tier 3 (5 units)
12/6/2011 Stanton Street, Tier 3 (4 units)
11/4/2011 Lincoln Juarez, Tier 2 (6 units)
10/18/2011 Veterans International Bridge, Tier 2 (3 units)
9/20/2011 DeConcini, Tier 3 (2 units)
9/13/2011 Hidalgo, Tier 2 (6 units)
9/13/2011 Pharr, Tier 2 (3 units)
9/7/2011 Anzalduas, Tier 1 (4 units)

2/8/2011 Douglas, Tier 3 (2 units)
Total units deployed - 110



License plate scanners: Useful tools, but what about all that data?

- By Kathleen Hickey
- Aug 01, 2012

Police around the country have been making increasing use of automatic license plate recognition (ALPR) systems, which combine optical character recognition with database storage and matching to help catch criminals, solve crimes and finding missing people.

In fact, their use is becoming so widespread that some organizations are raising privacy concerns.

ALPRs use a camera and OCR to read and photograph license plates as a police car travels down the road or cruises a parking lot. A computer compares the information collected with a national database; when a match is found the officer receives an alert on his/her computer, which shows the vehicle owner and nature of the potential problem.

The devices can use existing closed-circuit television, road-rule enforcement cameras, infrared cameras or cameras specifically designed for the task. Some can store a photograph of the driver, noted a [Wikipedia entry](#).

ALPRs are also known by various other terms, including automatic vehicle identification (AVI); car plate recognition (CPR); license-plate recognition (LPR); lecture automatique de plaques d'immatriculation (LAPI) and automatic number plate recognition (ANPR).

The cameras were designed to help locate stolen cars, wanted criminals and vehicles involved in Amber or Silver alerts. They are also used as a method of toll collection.

Police have been enthusiastic about the technology, which is becoming more widespread as prices for the devices drop. Two of the latest to install the technology are police in Des Moines and Sioux City, Iowa, reported the [Des Moines Register.com](#).

Police in Sioux City will begin using the technology in about a month; Des Moines will be adding it in the fall. The program debuted in Iowa in Polk County police vehicles last year.

"We're just trying to make it right for everyone on the street," said Polk County Sheriff's Deputy Jeff Rullman in the article. "The number of plates this thing will read on a daily basis compared to what an officer can -- it's no comparison. It's not uncommon to have this thing run 6,000, 7,000 plates" during an eight-hour shift on a busy Des Moines street, he added.

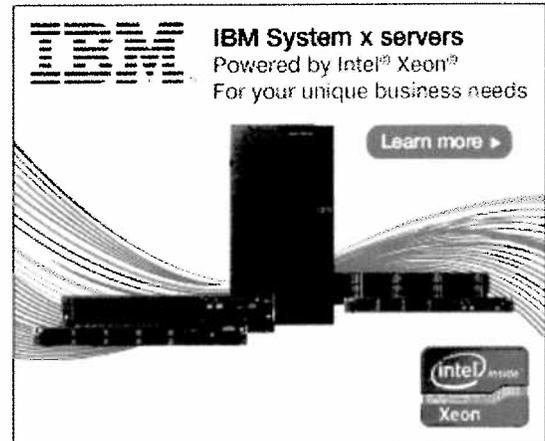
Polk County obtained the devices gratis via a nearly \$26,000 grant from the Justice Department. The police department will probably apply for additional funds for more equipment, said Rullman.

Large cities have been using the technology for a while. In Washington, D.C., for example, a network of ALPRs collects 1,800 images per minute, which are added to a database of people's movements around the city, the [Washington Post](#) has [reported](#).

The storage of those images is what has gotten the attention of the American Civil Liberties Union. The ACLU is questioning whether these gadgets will be used in a way that will create an Orwellian state.

In late July, ACLU affiliates in 38 states sent requests to local police departments and state agencies, asking how they will be using the readers to track and record Americans' movements. In addition, the national organization and the ACLU of Massachusetts filed Freedom of Information Act requests with the Justice, Homeland Security and Transportation departments to learn how the federal government is funding the use of ALPRs and how the agencies themselves will be using the technology.

"When used in a narrow and carefully regulated way, ALPRs can help police recover stolen cars and arrest people with outstanding warrants. Unfortunately, law enforcement agencies are increasingly moving towards a 'keep everything, share widely' formula concerning ALPR data," with many police departments storing location information of millions of motorists, not just those suspected of criminal activity," the ACLU said in a recent [blog](#) on the topic.



"Only two states (New Hampshire and Maine) have passed legislation barring the retention of 'non-hit' plate data for extended periods," the ACLU said. "On the other hand, we know for certain that some departments are eagerly engaging in this surreptitious data collection. As license plate location data accumulates, the system ceases to be simply a mechanism enabling efficient police work and becomes a warrantless tracking tool, enabling retroactive surveillance of millions of people."

But are these popular yet controversial devices more effective than current methods? According to a blog post at [Reason.com](#), a 2010 study by George Mason University's Center for Evidence-Based Crime Policy found that "[o]ver a third of large police agencies have already adopted [license plate recognition]" even though there's been little discussion of its use or of community concerns, and "the question still remains as to whether this technology is more effective in reducing, preventing or even detecting crime."

Even Polk County's Rullman conceded that he doesn't really know how many law breakers have been identified using the technology.

Interestingly, the concern of the ACLU -- storing information on non-criminals for indefinite periods -- appears to be seen as a bonus by law enforcement. Des Moines police spokesman Christopher Scott noted that if a license plate is later tied to a child abduction, database information on the plate could be used to potentially track the abductor.

"People get freaked out about running plates and having banks of information," he said in The Des Moines Register. "What we're doing is basically putting in our storage bag a license plate, and if we search for it we can find that information. If we're not searching for it, we'll never find that information."

About the Author

Kathleen Hickey is a freelance writer for the 1105 Government Information Group.

Reader Comments

Thu, Aug 2, 2012

Our PD installed the system and tried to make it work. It didn't. I think they asked for their money back. Lots of technical issues to overcome.

Thu, Aug 2, 2012 Charels Kerr United States

"...If we're not searching for it, we'll never find that information." That is the scary part... they aren't searching for me so they'll never find me. Until they do search for me. And then they will find me. It was said best in the article with the retroactive search. Connecticut has it right with ditching all the data that ins't a positive hit.



UNDERSTANDING THE TRUE COST OF DATA ENCRYPTION

Download this ground breaking study by the Ponemon Institute

• [CLICK HERE TO DOWNLOAD THE PONEMON STUDY](#)



© 1996-2011 1105 Media, Inc. All Rights Reserved.

The Washington Post

[Back to previous page](#)



How to Quickly Boost Your Testosterone for Increased Performance



Why Penny Stocks are the Road to Riches for Many Small Investors



This Company Really is Selling New iPads for as Low as \$40 - See How

License plate readers: A useful tool for police comes with privacy concerns

By [Allison Klein](#) and [Josh White](#), Published: November 19, 2011

An armed robber burst into a Northeast Washington market, scuffled with the cashier, and then shot him and the clerk's father, who also owned the store. The killer sped off in a silver Pontiac, but a witness was able to write down the license plate number.

Police figured out the name of the suspect very quickly. But locating and arresting him took a little-known investigative tool: a vast system that tracks the comings and goings of anyone driving around the [District](#).

[Scores of cameras](#) across the city capture 1,800 images a minute and download the information into a rapidly expanding archive that can pinpoint people's movements all over town.

Police entered the suspect's license plate number into that database and learned that the Pontiac was on a street in Southeast. Police soon arrested Christian Taylor, who had been staying at a friend's home, and charged him with two counts of first-degree murder. His trial is set for January.

More than 250 cameras in the District and its suburbs scan license plates in real time, helping police pinpoint stolen cars and fleeing killers. But the program quietly has expanded beyond what anyone had imagined even a few years ago.

With virtually no public debate, police agencies have begun storing the information from the cameras, building databases that document the travels of millions of vehicles.

Nowhere is that more prevalent than in the District, which has more than one plate-reader per square mile, the highest concentration in the nation. Police in the Washington suburbs have dozens of them as well, and local agencies plan to add many more in coming months, creating a comprehensive dragnet that will include all the approaches into the District.

“It never stops,” said Capt. Kevin Reardon, who runs Arlington County’s plate reader program. “It just gobbles up tag information. One of the big questions is, what do we do with the information?”

Police departments are grappling with how long to store the information and how to balance privacy concerns against the value the data provide to investigators. The data are kept for three years in the District, two years in Alexandria, a year in Prince George’s County and a Maryland state database, and about a month in many other suburban areas.

“That’s quite a large database of innocent people’s comings and goings,” said Jay Stanley, senior policy analyst for the American Civil Liberties Union’s technology and liberty program. “The government has no business collecting that kind of information on people without a warrant.”

But police say the tag readers can give them a critical jump on a child abductor, information about when a vehicle left — or entered — a crime scene, and the ability to quickly identify a suspected terrorist’s vehicle as it speeds down the highway, perhaps to an intended target.

Having the technology during the Washington area sniper shootings in 2002 might have stopped the attacks sooner, detectives said, because police could have checked whether any particular car was showing up at each of the shooting sites.

“It’s a perfect example of how they’d be useful,” said Lt. T.J. Rogers, who is responsible for the 26 tag readers maintained by the Fairfax County police. “We see a lot of potential in it.”

The plate readers are different from red-light or speed cameras, which issue traffic tickets and are tools for deterrence and enforcement. The readers are an investigative tool, capturing a picture of every license plate that passes by and instantly analyzing them against a database filled with cars wanted by police.

Police can also plug any license plate number into the database and, as long as it passed a camera, determine where that vehicle has been and when. Detectives also can enter a be-on-the-lookout into the database, and the moment that license plate passes a detector, they get an alert.

It’s that precision and the growing ubiquity of the technology that has libertarians worried. In Northern Virginia recently, a man reported his wife missing, prompting police to enter her plate number into the system.

They got a hit at an apartment complex, and when they got there, officers spotted her car and a note on her windshield that said, in essence, “Don’t tow, I’m visiting apartment 3C.” Officers knocked on the door of that apartment, and she came out of the bedroom. They advised her to call her husband.

A new tool in the arsenal

Even though they are relatively new, the tag readers, which cost about \$20,000 each, are now as widely used as other high-tech tools police employ to prevent and solve crimes, including surveillance cameras, gunshot recognition sensors and mobile fingerprint scanners.

License plate readers can capture numbers across four lanes of traffic on cars zooming up to 150 mph.

“The new technology makes our job a lot easier and the bad guys’ job a lot harder,” said D.C. Police Chief Cathy Lanier.

The technology first was used by the postal service to sort letters. Units consist of two cameras — one that snaps digital photographs and another that uses an optical infrared sensor to decipher the numbers and letters. The camera captures a color image of the vehicle while the sensor “reads” the license plate and transfers the data to a computer.

When stored over time, the collected data can be used instantaneously or can help with complex analysis, such as whether a car appears to have been followed by another car or if cars are traveling in a convoy.

Police also have begun using them as a tool to prevent crime. By positioning them in nightclub parking lots, for example, police can collect information about who is there. If members of rival gangs appear at a club, police can send patrol cars there to squelch any flare-ups before they turn violent. After a crime, police can gather a list of potential witnesses in seconds.

“It’s such a valuable tool, it’s hard not to jump on it and explore all the things it can do for law enforcement,” said Kevin Davis, assistant chief of police in Prince George’s County.

The readers have been used across the country for several years, but the program is far more sophisticated in the Washington region. The District has 73 readers; 38 of them sit stationary and the rest are attached to police cars. D.C. officials say every police car will have one some day.

The District’s license plate cameras gather more than a million data points a month, and officers make an average of an arrest a day directly from the plate readers, said Tom Wilkins, executive director of the D.C. police department’s intelligence fusion division, which oversees the plate reader program. Between June and September, police found 51 stolen cars using the technology.

Police do not publicly disclose the locations of the readers. And while D.C. law requires that the footage on crime surveillance cameras be deleted after 10 days unless there’s an investigative reason to keep it, there are no laws governing how or when Washington area police can use the tag reader technology. The only rule is that it be used for law enforcement purposes.

“That’s typical with any emerging technology,” Wilkins said. “Even though it’s a tool we’ve had for five years, as it becomes more apparent and widely used and more relied upon, people will begin to scrutinize it.”

Legal concerns

Such scrutiny is happening now at the U.S. Supreme Court with a related technology: GPS surveillance. At issue is whether police can track an individual vehicle with an attached GPS device.

Orin Kerr, a law professor at George Washington University who has been closely watching the

Supreme Court case, said the license plate technology probably would pass constitutional muster because there is no reasonable expectation of privacy on public streets.

But, Kerr said, the technology's silent expansion has allowed the government to know things it couldn't possibly know before and that the use of such massive amounts of data needs safeguards.

"It's big brother, and the question is, is it big brother we want, or big brother that we don't want?" Kerr said. "This technology could be used for good and it could be used for bad. I think we need a conversation about whether and how this technology is used. Who gets the information and when? How long before the information is deleted? All those questions need scrutiny."

Should someone access the database for something other than a criminal investigation, they could track people doing legal but private things. Having a comprehensive database could mean government access to information about who attended a political event, visited a medical clinic, or went to Alcoholics Anonymous or Planned Parenthood.

Maryland and Virginia police departments are expanding their tag reader programs and by the end of the year expect to have every major entry and exit point to the District covered.

"We're putting fixed sites up in the capital area," said Sgt. Julio Valcarcel, who runs the Maryland State Police's program, which now has 19 mobile units and one fixed unit along a major highway, capturing roughly 27 million reads per year. "Several sites are going online over the winter."

Some jurisdictions store the information in a large networked database; others retain it only in the memory of each individual reader's computer, then delete it after several weeks as new data overwrite it.

A George Mason University study last year found that 37 percent of large police agencies in the United States now use license plate reader technology and that a significant number of other agencies planned to have it by the end of 2011. But the survey found that fewer than 30 percent of the agencies using the tool had researched any legal implications.

There also has been scant legal precedent. In Takoma Park, police have two tag readers that they have been using for two years. Police Chief Ronald A. Ricucci said he was amazed at how quickly the units could find stolen cars. When his department first got them, he looked around at other departments to see what kind of rules and regulations they had.

"There wasn't much," Ricucci said. "A lot of people were using them and didn't have policies on them yet."

Finding stolen cars faster

The technology first came to the Washington region in 2004 as a pilot program. During an early test, members of the Washington Area Vehicle Enforcement Unit recovered eight cars, found 12 stolen license plates and made three arrests in a single shift. Prince George's police bought several units to help combat the county's crippling car theft and carjacking problem. It worked.

"We recover cars very quickly now. In previous times that was not the case," said Prince George's Capt. Edward Davey, who is in charge of the county's program. "Before, they'd be dumped on the side of the road somewhere for a while."

Now Prince George's has 45 units and is likely to get more soon.

"The more we use them, the more we realize there's a whole lot more on the investigative end of them," Davey said. "We are starting to evolve. Investigators are starting to realize how to use them."

Arlington police cars equipped with the readers regularly drive through the parking garage at the Pentagon City mall looking for stolen cars, checking hundreds of them in a matter of minutes as they cruise up and down the aisles. In Prince William County, where there are 12 mobile readers, the units have been used to locate missing people and recover stolen cars.

Unlike in the District, in most suburban jurisdictions, the units are only attached to police cars on patrol, and there aren't enough of them to create a comprehensive net.

Virginia State Police have 42 units for the entire state, most of them focused on Northern Virginia, Richmond and the Tidewater area, and as of now have no fixed locations. There is also no central database, so each unit collects information on its own and compares it against a daily download of wanted vehicles from the FBI and the state.

But the state police are looking into fixed locations that could capture as many as 100 times more vehicles, 24 hours a day, with the potential to blanket the interstates.

"Now, we're not getting everything — we're fishing," said Sgt. Robert Alessi, a 23-year veteran who runs the state police's program. "Fixed cameras will help us use a net instead of one fishing pole with one line in the water waiting to get a nibble."

Beyond the technology's ability to track suspects and non-criminals alike, it has expanded beyond police work. Tax collectors in Arlington bought their own units and use the readers to help collect money owed to the county. Chesterfield County, in Virginia, uses a reader it purchased to collect millions of dollars in delinquent car taxes each year, comparing the cars on the road against the tax rolls.

Police across the region say that they are careful with the information and that they are entrusted with many pieces of sensitive information about citizens, including arrest records and Social Security numbers.

"If you're not doing anything wrong, you're not driving a stolen car, you're not committing a crime," Alessi said, "then you don't have anything to worry about."

RELATED NEWS:

[Graphic: Who has LPR cameras and how long do police hold on to information?](#)

MORE NEWS FROM POSTLOCAL:

[Even as Pr. George's workers endure pay freeze, raises planned for leaders](#)

[Thieves target high-end eyewear stores](#)

[Federal agency parties take a holiday](#)

Man injured in jump from Va. parking garage

Sponsored Links

GTSO Stock on Fire

Traders Excited About Investment's Dynamite Performance, Buy Now!
www.GTSOResources.com

What is Your Flood Risk?

Protect your home from floods. Get your flood risk profile today.
www.floodsmart.gov

QUAN Stock Exploding

Price Jumps 36% & Volume Skyrockets - Invest Now!
www.QuantumInnovators.com

Buy a link here

© The Washington Post Company

