VIRGINIA: IN THE CIRCUIT COURT OF THE COUNTY OF FAIRFAX

HARRISON NEAL,

Plaintiff,

v.

Civil No.

FAIRFAX COUNTY POLICE

DEPARTMENT and COLONEL EDWIN C.

ROESSLER, JR., Chief of Police, Fairfax

County Police Department.

)

Defendants.

COMPLAINT

Introduction

1. This is an action for an injunction and/or writ of mandamus under the Government Data Collection and Dissemination Practices Act, Va. Code §§ 2.2-3800 et seq. (the "Data Act"), a statute that was designed to prevent government agencies from unnecessarily collecting, storing, or disseminating the personal information of individuals. Defendants Fairfax County Police Department (FCPS) and its Chief of Police have violated the statute by using Automated License Plate Readers (ALPRs) to scan tens or hundreds of thousands of license plates of vehicles not suspected of any involvement in criminal activity, along with the date and location at which the plate was scanned, storing the data for one year, and sharing the data with other law enforcement agencies in the District of Columbia metropolitan area. The defendants' massive ALPR database allows the department, and the law enforcement agencies with which it shares data, to determine whether particular vehicles have been in the vicinity of, for example, particular churches, political rallies, or doctors' offices, undermining the privacy of the drivers of those vehicles. The plaintiff, a resident of Fairfax County whose license plate data has been

collected at least twice by the defendants, respectfully requests an injunction and/or writ of mandamus prohibiting the defendants from continuing to violate the Data Act.

Jurisdiction and Venue

2. Jurisdiction and venue are proper in this Court pursuant to Va. Code § 2.2-3809, because plaintiff Harrison Neal resides in Fairfax County and because defendant Fairfax County Police Department has a place of business in Fairfax County.

Parties

- 3. Plaintiff Harrison Neal is an adult resident of Fairfax County, Virginia.
- 4. Defendant Fairfax County Police Department (FCPD) is an agency of Fairfax County, Virginia, and the primary law enforcement agency for Fairfax County, Virginia.
- 5. Defendant Colonel Edwin C. Roessler, Jr., is the Chief of Police Fairfax County Police Department. As such, he is in command of the FCPD and makes rules and regulations concerning the operation of the FCPD and the conduct of its officers and employees. Fairfax Cnty. Charter Sec. 10.3.

Factual Allegations

ALPRs

- 6. An ALPR (sometimes referred to as an "LPR") is a device that automatically records every license plate that comes into its field of vision, along with the date, time, and location at which the record was made. It is capable of recording thousands of license plates per minute. ALPRs are often mounted on police vehicles or on stationary objects.
- 7. Broadly speaking, law enforcement agencies use ALPRs in two ways. First, the agency may maintain a "hot list" of license plate numbers, which may include the plates of vehicles that have been reported missing or that are suspected of involvement in a crime. Every

time the ALPR scans a license plate, the scan is automatically checked against the hot list, so that target vehicles may be quickly identified. The plaintiff does not challenge this type of use of ALPRs, which is sometimes called "active" use.

8. Second, law enforcement may save the data associated with every license plate scan and store it in a large database. The database may later be queried to determine whether a particular vehicle was seen at a particular date and time at a particular place. This use of ALPRs, sometimes called "passive," violates the Data Act.

Defendants' Use of ALPRs

- 9. Since at least 2010, the Fairfax County Police Department has possessed one or more ALPRs. The equipment was provided to the FCPD by Arlington County, Virginia as part of a grant from the United States Department of Homeland Security. Arlington County was the administrator of the grant, which was intended to provide ALPR equipment to participating law enforcement agencies in the Washington, D.C. area.
- 10. Pursuant to FCPD SOP 11-039, adopted in January 2010 and, upon information and belief, still in effect, the FCPD uses its ALPRs in both an "active" and a "passive" manner. (A copy of SOP 11-039 is attached as Exhibit A and is fully incorporated herein.)
- 11. With respect to the "passive" use of ALPRs, the FCPD's policy states: "ALPR generated data will be maintained on the server for a period not to exceed 365 days without specific authorization of the Chief of Police. The purpose of the retention period is to increase protection of the community by providing an investigative tool to aid in the detection or investigation of terrorism or a series of related crimes."
- 12. Additionally, the FCPD is a party to a Memorandum of Understanding ("MOU") among an unknown number of law enforcement agencies in the Washington, D.C. area

pertaining to the sharing of ALPR data. Under the MOU, each participating agency agrees to allow every other participating agency to access its ALPR database for law enforcement purposes.

- 13. On or about May 9, 2014, plaintiff Neal submitted a request to the FCPD seeking all ALPR records related to a particular license plate number for a vehicle that he owns. In response, on May 15, 2014, the FCPD sent Neal a letter stating that "[w]ithin the last 364 days, your tag was read twice by our ALPR system."
- 14. The response from FCPD also included two sheets of paper, each of which had two pictures of Neal's vehicle and a chart indicating the time, date at which the photographs were taken. Each chart also includes the words "Mason 4866." Upon information and belief, "Mason 4866" designates the specific ALPR device that took the photographs. The response also included a map on which a particular location is marked, which Neal assumes is the location at which the device is or was mounted. (The entire response from FCPD is attached hereto as Exhibit B and is fully incorporated herein.)
- 15. The location depicted on the map included in the FCPD response is one that Neal drives past frequently in the course of his employment and for other purposes.

Application of the Data Act to Defendants' Use of ALPR

- 16. The Data Act governs the collection, storage, and dissemination of "personal information" by government agencies.
- 17. The Data Act defines "agency" in relevant part as "any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity... of any unit of local government including... counties... and the departments thereof." Va. Code § 2.2-3801. FCPD is an "agency" as defined by the Data Act.

- 18. The Data Act defines "personal information" in relevant part as information that "describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record." Va. Code § 2.2-3801.
- 19. License plate numbers are "personal information" under the Data Act because they are indexed to vehicle owners' social security numbers, driver's license numbers, addresses, vehicle liens, dates of birth, and photographs in Department of Motor Vehicles databases readily accessible to law enforcement agencies.
- 20. The Data Act requires agencies that collect personal information to adhere to certain "principles of information practice," including the following:
 - Information shall not be collected unless the need for it has been clearly established in advance.
 - Information shall be appropriate and relevant to the purpose for which it has been collected.
 - There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

Va. Code 2.2-3800(C)(2), (3), (9). None of these conditions are met with respect to the defendants' "passive" use of ALPRs.

- 21. The Data Act also requires agencies to adhere to certain administrative requirements for information systems including personal information, including the following:
 - Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;
 - Collect information to the greatest extent feasible from the data subject directly;

- Maintain a list of all persons or organizations having regular access to personal information in the information system;
- Maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained,

Upon information and belief, none of these conditions are met with respect to defendants' database of ALPR information. Va. Code § 2.2-3803(A)(1), (2), (5), (6), (7).

- 22. The Data Act sets forth certain rights of "data subjects," defined as "an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system." Va. Code § 2.2-3801.
 - 23. Harrison Neal is a "data subject" as defined by the Data Act.
- 24. Among other things, agencies maintaining personal information must "[g]ive notice to a data subject of the possible dissemination of part or all of this information to another agency, nongovernmental organization or system not having regular access authority, and indicate the use for which it is intended . . ." Va. Code § 2.2-3806(A)(2). Neal did not receive such notice.
- 25. The Data Act provides that "[e]very agency shall make report of the existence of any information system that it operates or develops that shall include a description of the nature of the data in the system and purpose for which it is used. An inventory listing or similar display of the information shall be made available for inspection by the general public in the office of the head of each agency. Copies of the information shall be provided upon request and a fee shall be charged for them sufficient to cover the reasonable costs of reproduction." Va. Code § 2.2-3807. Upon information and belief, no such report exists with respect to the defendants' database of ALPR information.

- 26. On February 13, 2013, then-Attorney General of Virginia Kenneth T. Cuccinelli, II, issued a legal opinion on the use of ALPRs by Virginia law enforcement agencies (the "Legal Opinion"). The Legal Opinion was issued in response to a request by the Superintendent of the Virginia State Police, Colonel W.S. Flaherty. A copy of the Legal Opinion is attached hereto as Exhibit C.
- 27. The Legal Opinion advises Colonel Flaherty that the "active" use of ALPRs is permissible under the Data Act, but that the "passive" use of the technology is prohibited by that statute.
- 28. The Legal Opinion notes that data collected with ALPRs is "personal information" as defined by the Data Act. Additionally, ALPR data collected and stored in a "passive" manner does not fall within the Data Act's exemption for information systems "[m]aintained by . . . police departments of cities, counties, and towns . . . and that deal with investigations and intelligence gathering relating to criminal activity." Va. Code § 2.2-3802(7).
- 29. The Legal Opinion further advises that the "passive" collection and storage of ALPR information violates the Data Act because the need for such information has not been "clearly established in advance," as required under Va. Code Va. Code 2.2-3800(C)(2). Rather, the information's "future value to any investigation of criminal activity is wholly speculative."
- 30. Following the issuance of the Legal Opinion, the Virginia State Police ceased using its ALPR equipment for "passive" data collection, and purged its database of any information so collected that was not directly related to a criminal investigation.
- 31. Notwithstanding the Legal Opinion and the actions of the Virginia State Police in response to the Legal Opinion, the defendants and other Northern Virginia law enforcement agencies who are parties to the MOU continued to use their ALPR equipment for the purpose of

"passive" data collection, to store such information in databases, and to make such information available to other parties to the MOU.

Cause of Action
Violation of the Data Act, Va. Code §§ 2.2-3800 et seq.

32. Plaintiffs are "aggrieved persons" entitled to relief pursuant to Va. Code § 2.2-

3809.

33. The defendants' collection, storage, and dissemination of "passively" collected

ALPR data, including personal information about the plaintiffs that has been, and likely will be

in the future, collected and maintained in defendant's ALPR database, violates the Data Act.

Request for Relief

For the foregoing reasons, plaintiffs request the following relief pursuant to Va. Code § 2.2-3809:

A. An injunction and/or a writ of mandamus prohibiting the defendants from using ALPR equipment for the "passive" collection of license plate information, and requiring the defendants to purge all databases containing all "passively" collected license plate information;

B. Plaintiffs' costs and reasonable attorneys' fees for pursuing this action; and

C. Such other relief as this Court deems just and proper.

Dated: May 4, 2015

Respectfully submitted:

Rebecca K. Glenberg (VSB No. 44099)

Hope R. Amezquita (VSB No. 74629)

American Civil Liberties Union Foundation of Virginia, Inc.

701 E. Franklin St., Suite 1412

Richmond, VA 23219

(804) 644-8080 Facsimile: (804) 649-2733 rglenberg@acluva.org hamezquita@acluva.org

RULE 3:25(B) CERTIFICATE

Pursuant to Rule 3:25(B) of the Rules of the Supreme Court of Virginia, counsel for plaintiff certifies that plaintiff's claim for attorneys' fees arises from the Government Data Collection and Dissemination Practices Act, Va. Code § 2.2-3809, which provides: "In the case of any successful proceeding by an aggrieved party, the agency enjoined or made subject to a writ of mandamus by the court shall be liable for the costs of the action together with reasonable attorneys' fees as determined by the court."

Dated: May 4, 2015

Rebecca K. Glenberg Attorney for Plaintiff TITLE: Automatic License Plate Readers

SOP NUMBER: 11-039

EFFECTIVE DATE: 01-01-11

REPLACES/RESCINDS:



I. PURPOSE

The purpose of this SOP is to establish specific procedures pertaining to the operating guidelines, maintenance, data retention, storage, access, release of information, and the responsibilities relevant to the use and operation of Automatic License Plate Readers (ALPR) and associated data. The ALPR Program will be housed and coordinated by the Commander of Patrol Bureau Division I, with technical assistance from the Information Technology Bureau and Resource Management Bureau.

II. POLICY

The use of ALPR technology is intended as a tool for law enforcement to identify stolen license plates and vehicles or any vehicle identified as having a specific interest to law enforcement. It shall be the policy of the Fairfax County Police Department to use ALPR technology for law enforcement functions that will detect criminal activity and promote the health, safety and welfare of Fairfax County residents and visitors. This technology shall be used in a manner consistent with legal and constitutional limitations, privacy concerns and the highest ethical standards.

III. DEFINITIONS

ALARM (aka hit): A positive indication or "hit" by audio and/or visual signal, of a potential match between data on the "hot list" and a license plate scanned by the ALPR System. An alarm is NOT conclusive confirmation that a license plate or vehicle is wanted, but an indicator that additional investigation is warranted.

CD-R/Compact Disc Recordable: A format that allows data to be recorded to a blank CD-R disc one time.

ELSAG Operations Center Software: Manages all data collected by ALPR units for ease of analysis. The software seamlessly monitors all ALPR units to ensure each unit is up to date with the most accurate information. The software also downloads data from the ALPR unit to the server automatically.



DOWNLOAD: Transfer of data from the Virginia State Police database consisting of license plate associated data.

HOT LIST: A "hot list" is a list of targeted license plate numbers and partial plate numbers that are uploaded to ALPR units on a daily basis.

UPLOAD: Transfer of data from ALPR units to storage on the ALPR server.

IV. OVERVIEW

Each day the Virginia State Police generates a "hot list" containing all active stolen license plates and vehicles entered into NCIC/VCIN. This information is available to authorized law enforcement personnel via a secure Web site. The "hot list" is imported either automatically through a server or manually by the end user into the License Plate Reader System. Wanted vehicles may also be entered into the ALPR manually by the end user as circumstances dictate.

The ALPR scans license plates and compares them to data provided by the Virginia State Police. The ALPR software runs in the background of the MCT, and automatically alerts the police operator to a potential stolen vehicle or license plate. The ALPR maintains the date, time and location of each license plate it scans.

V. PROCEDURES

The following procedural guidelines have been established to ensure the proper use of the Automatic License Plate Reader System.

A. Operation of the ALPR System shall only be performed by those authorized employees who have successfully completed the Fairfax County Police Department's approved training for ALPR devices. All operators shall receive training prior to using the ALPR System.

Training will be conducted in a "train the trainer" format. The Patrol Bureau will arrange for at least one annual "train the trainer" class. Commanders will be responsible for ensuring employees under their respective command receive proper training. Training documentation will be forwarded to the Fairfax County Criminal Justice Academy.

B. A dedicated server for the ALPR System and software will automatically update the ALPR "hot list" on the MCTs as they become available from the Virginia State Police server.

VI. INTERNAL DATA ACCESS, STORAGE, AND RETENTION

- A. The Patrol Bureau will have overall responsibility of the collection, storage, dissemination, and retention of non-evidentiary data associated with the program. Technical assistance will be provided by the Information Technology Bureau (ITB) or the vendor (ELSAG North America 1-866-967-4900).
- B. Access to stored ALPR records shall be for a specific investigative or patrol purpose(s). ALPR data is considered an official record and shall be handled as such in accordance with Regulation 204.4. Improper or misuse of any ALPR data is grounds for disciplinary action. All data collected by the ALPR System is the sole property of the Fairfax County Police Department and shall not be released without authorization from the Chief of Police or his designee.
- C. Crime analysts and sworn employees trained in the use of the ELSAG Operations Center software shall have full access to ALPR data to conduct analysis of data and processing requests for data from any Police Department employee having a legitimate law enforcement request. Any disputes which result from a request will be resolved by a supervisor. The Department has limited licenses for the ELSAG Operations Center software, so only select terminals throughout the agency will have access to the program.
- D. In those circumstances when data is identified as having evidentiary value, a supervisor shall review the facts and determine if the data should be saved. If the reviewing supervisor determines it is reasonable to believe the data has evidentiary value, he will authorize the downloading of the applicable data from the ALPR server onto a CD-R for filing.
- E. The Master Copy CD-R disc containing the original ALPR data and images will be placed in a paper CD sleeve with the following information:
 - Case number
 - Date
 - Location of event
 - Event type
 - · Investigating officer's name
 - Brief description of data extracted
- F. The sleeved CD-R will be placed in the departmental standard 9"x12" stamped envelope with all required information indicated above. The sealed envelope containing the sleeved CD-R will be submitted directly to the Record Room for filing. Nothing in this policy shall preclude the investigating officer or detective from making one additional copy for his case file.

- G. It shall be the responsibility of the operator to ensure the most current "hot list" available has been transferred into the ALPR prior to its use. A "hot list" more than 24 hours old may be utilized.
- H. A "hot list" more than 72 hours old shall not be utilized.
- I. An "ALARM" is NOT in and of itself sufficient reasonable suspicion to make a stop or effect an arrest without further verification. After receiving an audible or visual alarm of a potential stolen vehicle or license plate the information shall be verified prior to taking any law enforcement action. The operator must use due diligence in verifying any alarms received when utilizing a hot list more than 24 hours old. Alarm verifications will be accomplished in a two step process.
 - 1. The ALPR operator shall visually verify the subject tag with the data displayed on the ALPR screen (e.g., same state, characters).
 - Once a visual comparison is confirmed, the operator shall verify the hit is still
 active by running the information via MCT or voice a request for a
 NCIC/VCIN through DPSC.

Nothing shall preclude officers acting on other indicators to develop reasonable suspicion based on training and experience.

- J. Stolen vehicle or license plate responses from NCIC/VCIN shall be confirmed by Teletype in accordance with established procedures as soon as practical.
- K. At the discretion of the ALPR operator, additional information may be entered into the ALPR System at any time. The reason for the entry shall be included in the "note" portion of the entry mask (e.g., stolen vehicle, missing person, abduction, Amber Alert, robbery suspect). The name of the investigating officer or detective with a 24/7 contact number shall also be included. Officers entering information are responsible for ensuring that all custom manual inputs have a specific criminal investigative or patrol use. The data will be overwritten automatically by the next scheduled update of the "hot list" from the Virginia State Police.
- After completing a manual entry the operator should query the ALPR data to determine if the license plate was scanned previously.
- M. All contacts resulting from ALPR use shall be documented as appropriate in the I/Leads Records Management System. In rare cases where documentation is not otherwise required, officers shall enter comments into the event using the COMMENT button from the event screen in I/Mobile.

- N. Any data extracted from the ALPR server to be retained as evidence shall be documented in the Incident Module or as a supplement to an existing case in I/LEADS.
- O. ALPR generated data will be maintained on the server for a period not to exceed 365 days without specific authorization of the Chief of Police. The purpose of the retention period is to increase protection of the community by providing an investigative tool to aid in the detection or investigation of terrorism or series of related crimes.

VII. EXTERNAL DISSEMINATION of ALPR DATA

- A. Requests for secondary dissemination of information to outside law enforcement agencies shall be made to any commander who will either approve or deny the request based on the validity of the request which must be supported by a specific law enforcement need. Law enforcement agencies making a request for ALPR information must complete an ALPR Secondary Dissemination Form. Each form will contain the following information:
 - 1. The date and time the form was received
 - 2. The name and department of the requestor
 - 3. The purpose for which the ALPR data was requested including the agency's case number.
 - 4. A description of the ALPR data disseminated
 - 5. The date and time the information was released
 - 6. The identity of the individual to whom the information was released, including agency and contact information
 - 7. The name of the person processing the request
 - 8. The final status of the request (APPROVED or DENIED)
- B. The Crime Analyst Program director will maintain a secondary dissemination file which will contain completed ALPR Secondary Dissemination Forms and a copy of any information that was provided. ALPR Secondary Dissemination Forms and associated released file shall be retained electronically for a minimum of three years.
- C. Third party dissemination rules shall not apply to any law enforcement agency within the National Capital Region (NCR) having an MOU which grants access to Fairfax County ALPR files. Automatic data access will be facilitated by ITB for approved MOUs.

- D. Given special circumstances, Department authorized public and/or private entities offering assistance with regard to a high profile case or specific investigation may be provided corresponding ALPR data upon authorization from the Chief of Police or his designee, for the sole purpose of furthering the investigation. The data shall be destroyed by the receiving party when it becomes no longer relevant to the initial investigative need.
- E. All other requests for ALPR information shall be in accordance with the Virginia Freedom of Information Act (FOIA). FOIA requests are time sensitive and shall immediately be forwarded to the Inspections Division of the Internal Affairs Bureau.

VIII. DEPLOYMENT

- A. ALPR equipped vehicles may be used during routine patrol operations or for special operations by personnel properly trained in the use of ALPR. The role of the ALPR in special operations shall be outlined in the operations plan, and reviewed by a supervisor or commander.
- B. Operation of police vehicles equipped with ALPR shall be in accordance with General Order 501.1, Operation of Police Vehicles.
- C. ALPR Systems shall be inspected prior to operation.
- D. Supervisors should make every effort to deploy ALPR equipped vehicles, and when deployed, the units will be identified in I/NetDispatcher and on squad lineups.

IX. MAINTENANCE

- A. When ALPR equipment is removed from the vehicle for any reason it shall be placed in its protective case to prevent accidental damage.
- B. ALPR cameras shall be removed from vehicles prior to entering an automatic car washing facility.
- C. ALPR camera lenses may be cleaned with glass cleaner or mild soap and water.
- D. Damage to ALPR equipment shall be immediately reported to a first line supervisor. The supervisor shall document the damage in the form of a memorandum to the Logistics and Property Division director through his

- respective commander. Copies of all documentation shall be faxed to the Resource Management Bureau (RMB) by the end of shift.
- E. No alterations or repairs of any kind shall be made to ALPR equipment or software.
- F. The Logistics and Property Division of the RMB shall be notified of any ALPR equipment needing maintenance or repair. RMB will coordinate all maintenance and repair with the appropriate vendor.

X. ADMINISTRATIVE RESPONSIBILITIES

- A. The system administrator of the ELSAG Operations Center is housed in the Patrol Bureau. The functions of Diagnostics, Query / Statistics, Hot List Management, User Configuration, Software Management, Data Mining, Parameters Management and Role Management will be determined by Patrol Bureau.
- B. Server maintenance, software updates, and security of data are the responsibility of the Patrol Bureau with technical assistance from the Information Technology Bureau as needed.
- C. Functionality issues with ELSAG software on the MCT shall be examined by the CAD Tech Support at PSTOC.
- D. Installation, maintenance, and tracking of ALPR equipment are the responsibility of Logistics and Property Division director.
- E. The station logistics technicians will be responsible for coordinating the installation, tracking, maintenance; and coordinating the repair of software and hardware issues of ALPR equipment with the respective entities named above.

This SOP becomes effective January 1, 2011, and rescinds all previous rules and regulations pertaining to the subject.

Issued by:

Chief of Police



County of Fairfax, Virginia

To protect and enrich the quality of life for the people, neighborhoods, and diverse communities of Fairfax County

Colonel Edwin C. Roessler Jr. Chief of Police May 15, 2014

Harrison Neal 5125 Chowan Avenue Alexandria, Virginia 22312

Re: ALPR Information

Lt. Colonel Thomas Ryan Deputy Chief of Police for Administration

Our Re: 14-FOIA-186

Dear Mr. Neal:

Lt. Colonel
Ted Arnn
Deputy Chief of Police
for Investigations/
Operations Support

This letter is in response to your FOIA request received by this department on May 9, 2014 reference your vehicle with VA tag ADDCAR. Within the last 364 days your tag was read twice by our ALPR system. Your documents are enclosed.

Lt. Colonel Erin F. Schaible Deputy Chief of Police for Patrol Please remit the amount indicated on the invoice making your check payable to the "County of Fairfax". It should then be mailed to my attention at the below listed address.

To ensure your payment is properly credited please also enclose a copy of your invoice and reference our control number on your check. If I can be of further assistance please do not hesitate to contact me at (703) 246-2564 or FCPDFOIA@fairfaxcounty.gov.

Major Michael A. Kline Commander, Internal Affairs Bureau

Justin P. Palenscar, First Lieutenant

Internal Affairs Bureau

to alenson

Lieutenant Justin P. Palenscar Commander, Inspections Division JPP/aks

Sincerely.

User : Crime Analyst

Date : 2014/05/15 11:16:00

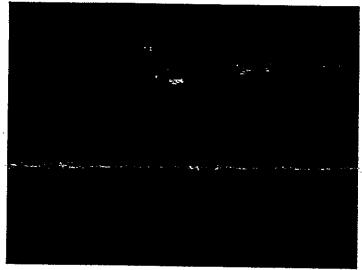


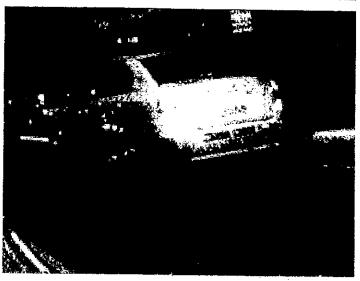


Gate .			Mason 4866					
Lane			1					
Transit Date and Time	11/05/2014 16:37:25	Vehicle type	79111	Transit status	Normal Transit			
License Plate			ADDCAR					
State			?					

User: Crime Analyst

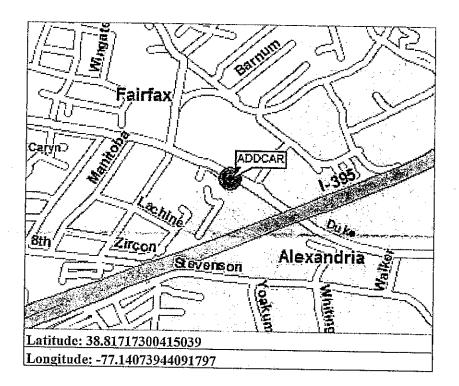
Date: 2014/05/15 11:35:51





Gate			Mason 4866			
Lane		,	0	······································		, <u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>
Transit Date and Time	26/04/2014 19:57:46	Vehicle type		Transit	status	Normal Transit
License Plate				ADD	CAR	
State					,	

INVOICE	Date Completed	E/4E/4	5/ 10/ 15		f Total Expense	\$11.41					\$11.41		Total Amount	\$0.30		\$0.30	
	Zip Code	00040	21022		Number of Hours	0.3				c	bTotal		Cost	\$0.10	Total	I Due	à 3
14-FOIA-186 FOIA 日本	Phone				Hourly Rate	\$38.0353					Research SubTotal				Services SubTotal	Grand Total Due	Total Amouitt Due By:
				Time	EIN	302193						ovided				<u>l ;</u>	a copy of . (Tax ID
County Police Department Internal Affairs Bureau 4100 Chain Bridge Road Fairfax, Virginia 22030	Address	5125 Chowan Avenua	Alexandria, Virginia	Research Time	nd Position Position	Crime Analyst III				Total Staff Besearch Time.	Comments	Services Provided	Description of Service(s) Provided		e Shipping Weights Over 116.)		Please make all Checks payable to: County of Fairfax, Virginia All payments should be mailed to the above listed address. Please include a copy of this satement so that your payment will be properly credited to your request. (Tax ID 54-0787833)
COUNT Interna 4100 C	Requestor:	Harrison Neal	Individual		Employee Name and Position Last Name	Abbott				F	COL		1	Charge per page copied (\$.10)	Comments (Note Sh		Please make all Checks pays County of Fairfax, Vii s should be mailed to the above listed addr t so that your payment will be properly cre 54-0787833)
			Type:				8 4	5	0 10	8			Qty	8			All payments s





COMMONWEALTH of VIRGINIA

Office of the Attorney General

Kenneth T. Cuccinelli, II Attorney General

February 13, 2013

900 East Main Street Richmond, Virginia 23219 804-786-2071 FAX 804-786-1991 Virginia Relay Services 800-828-1120 7-1-1

Colonel W.S. Flaherty Superintendent, Virginia Department of State Police Post Office Box 27472 Richmond, Virginia 23261-7472

Dear Colonel Flaherty:

I am responding to your request for an official advisory opinion in accordance with § 2.2-505 of the Code of Virginia.

Issues Presented

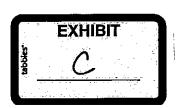
You inquire regarding the collection, maintenance, and dissemination of data collected from an automated license plate reader ("LPR"). Specifically, you ask whether the Government Data Collection and Dissemination Practices Act (the "Data Act") permits law enforcement agencies to collect, maintain, and disseminate LPR data. You also ask whether such data can be classified as "criminal intelligence information" under applicable Virginia law and thereby exempted from the Data Act's provisions.

Response

It is my opinion that the Data Act does not preclude law enforcement agencies from maintaining, using and disseminating personal information collected by an LPR, provided such data specifically pertains to investigations and intelligence gathering relating to criminal activity. It further is my opinion that data collected by an LPR may be classified as "criminal intelligence information" and thereby exempted from the Data Act's coverage only if the data is collected by or on behalf of the Virginia Fusion Intelligence Center, evaluated and determined to be relevant to criminal activity in accordance with, and maintained in conformance with the criteria specified in § 52-48 of the *Code of Virginia*. Finally, it is my opinion that data collected by an LPR that is not properly classified as "criminal intelligence information" and not otherwise relating directly to law enforcement investigations and intelligence gathering respecting criminal activity, is subject to the Data Act's strictures and prohibitions.

Background

LPRs use a combination of cameras and optical character recognition technology to read license plates. The camera captures an image of a license plate and the optical character recognition technology converts the image into data that can be searched against an existing database or the data may be stored for future use, along with the time, date, and location of the observation. You describe two methods to collect data utilizing an LPR: an "active" manner, whereby law enforcement collects, evaluates, and analyzes the LPR data in real time to determine the relevance to an ongoing case or emergency, and, alternatively, a



"passive" manner, whereby law enforcement collects unanalyzed data for potential future use if a need for the collected data arises respecting criminal or terroristic activities.

In your letter, you specifically describe these collection methods as follows:

Uses of LPR technology include searching for a specific plate number in cases involving vehicle larceny, abductions, wanted persons and in Amber/Senior/Blue Alerts. In these situations, the system allows law enforcement to process many more plates more accurately and much faster than they could through normal observation techniques. These systems are a vital tool in combating crime and protecting our most vulnerable populations.

The reason of this inquiry is another growing use of this technology. LPR systems can also be used to collect raw data. Whether the LPR reader is mobile or fixed, the data collected includes the image of the place, the time, date and precise location the license plate in question was captured by the system. This is accomplished passively and continuously. If the LPR system is on, it will capture and store the data for every license in plain view to the public it encounters. On a routine patrol, this may include thousands of license plate numbers and locations This can, and has been an invaluable tool in developing leads in terrorism investigations and criminal cases.

Applicable Law and Discussion

The Government Data Collection and Dissemination Practices Act¹ governs the collection, maintenance, and dissemination of personal information by government agencies.² The General Assembly enacted the Data Act in response to concerns about potentially abusive information-gathering practices by the government, including enhanced availability of personal information through technology.³ The Data Act serves to guide state agencies and political subdivisions in the collection and maintenance of personal information.⁴

The Data Act seeks to protect individual privacy, by placing strictures upon the governmental collection, maintenance, use and dissemination of personal information.⁵ "Personal information" includes

all information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued

¹ VA. CODE ANN. §§ 2.2-3800 through 2.2-3809 (2011).

² Your inquiry does not implicate the Fourth Amendment prohibition against unlawful search and seizure. See U.S. Const. amend IV. Fourth Amendment protections are triggered only when the state conducts a search or seizure in an area in which there is a "constitutionally protected reasonable expectation of privacy." New York v. Class, 475 U.S. 106 (1986). When there is no reasonable expectation of privacy, the Fourth Amendment is not implicated. See, e.g., United States v. Dionisio, 410 U.S. 1, 14 (1973) (no reasonable expectation of privacy in one's voice); United States v. Mara, 410 U.S. 19, 21 (1973) (no reasonable expectation of privacy in one's handwriting); California v. Greenwood, 486 U.S. 35, 37 (1988) (same as to trash left by the curb). Because there is no reasonable expectation of privacy to one's license plate in public places, the use of LPRs by law enforcement does not violate the Fourth Amendment; for "it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile." Class, 475 U.S. at 114 (finding no reasonable expectation of privacy in a VIN).

³ Hinderliter v. Humphries, 224 Va. 439, 443-44, 297 S.E.2d 684, 686 (1982). See § 2.2-3800(B) (listing General Assembly's findings leading to the Data Act's enactment).

⁴ See 2002 Op. Va. Att'y Gen. 3, 4.

⁵ Section 2.2-3800(B) and (C).

identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record [6]

Data collected utilizing LPR technology falls within this statutory definition, as, for example, it may assist in locating an individual data subject, documenting his movements, or determining his personal property holdings. The collection of such information may adversely affect an individual who, at some point in time, may be suspected of and or charged with a criminal violation. Accordingly, data collected by an LPR generally meets the definition of "personal information" and thus falls within the scope of the Data Act.

Therefore, the analysis of the issues you present must explore any exemptions to the Data Act's coverage that may be applied to data collected through LPR technology.

The Data Act's provisions afford an exemption for certain personal information systems that are "[m]aintained by the Department of State Police; the police department of the Chesapeake Bay Bridge and Tunnel Commission; police departments of cities, counties, and towns; and the campus police departments of public institutions of higher education "This exemption applies exclusively to information "that deal[s] with investigations and intelligence gathering relating to criminal activity[.]" 10

Clearly, data collected by an LPR in the active manner and maintained by such law enforcement entities relates directly to the immediate public safety threat of criminal activity. Thus, such data is exempted from the application of the Data Act by its specific terms.

With respect to LPR data collected to date in the passive manner, you note that it has proven "an invaluable tool in developing leads in terrorism investigations and criminal cases . . ., [including] in high profile cases like the Museum of the Marine Corps sniper case." Nevertheless, because no specific exemption applies to it, I must conclude that data so collected is subject to the Data Act's regulatory provisions.

At § 2.2-3800(C) of the *Code of Virginia*, and fundamental to the Data Act, the General Assembly enunciated several "principles of information practice to ensure safeguards for personal privacy". Among those principles is one particularly relevant to LPR data collected in the passive manner, stating that, "[i]nformation shall not be collected unless the need for it has been clearly established in advance."

You state that data collected by an LPR in the passive manner is considered "raw data", and is continuously recorded. It captures the "image of the place, the time, date and precise location the license plate in question[.]" You also explain that, "[f]he system only translates letters and numbers. This data is

⁶ Section 2.2-3801.

⁷ Readily attainable information may include the vehicle registrant's name, address, vehicle information, and potential lien status. The definition of "information system" also broadly encompasses records "containing personal information and the names, personal number, or other identifying particulars of a data subject." Section 2.2-3801. A "data subject" is "an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system." *Id.*

⁸ See § 2.2-3801.

⁹ Section 2.2-3802(7).

¹⁰ Id.

¹¹ Section 2.2-3800(C)(2).

then stored by the capturing agency and can be searched at a later date by an alphanumeric query to determine if, when and where a license plate matching the query was encountered."

On these facts I conclude that the need for such data has not been "clearly established in advance," so as to conform to the applicable principle of information practice. ¹² Its future value to any investigation of criminal activity is wholly speculative. Therefore, with no exemption applicable to it, the collection of LPR data in the passive manner does not comport with the Data Act's strictures and prohibitions, and may not lawfully be done. ¹³

With regard to your second inquiry, information that can be classified as "criminal intelligence information" also is expressly exempt from the application of the Data Act. This exemption is found in another part of the Code, one that relates to the Virginia Fusion Intelligence Center ("the fusion center"). Criminal intelligence information" is defined as "data that has been evaluated and determined to be relevant to the identification and criminal activity of individuals or organizations that are reasonably suspected of involvement in criminal activity. This definition, however, "shall not include criminal investigative files."

You ask whether data obtained through LPRs meets this definition. When construing a statute, the primary objective is "to ascertain and give effect to legislative intent," as expressed by the language used in the statute. Where the language of a statute is unambiguous, the courts are bound by the plain meaning of that language. Also, where a statute specifies certain things, the intention to exclude that which is not specified may be inferred, and "[courts] may not add to a statute language which the legislature has chosen not to include."

In defining the term "criminal intelligence information," the General Assembly specifically limited such information to "data that has been evaluated and determined to be relevant to the identification and criminal activity..." Thus, only information that has been both evaluated and determined to be relevant

¹² Section 2.2-3800(C)(2).

¹³ See §§ 2.2-3800(B) and (C), 2.2-3803(A), and 2.2-3809.

¹⁴ Section 52-48(A) (Supp. 2012).

¹⁵ See Chapter 11 of Title 52 of the Code of Virginia, VA. CODE ANN. §§ 52-47 through 52-49 (2009 & Supp. 2012). I note that the term "criminal intelligence information" is used only in this part of the Code, which deals exclusively with the Virginia Fusion Intelligence Center, and not with law enforcement practices more generally. The Virginia Fusion Intelligence Center is a multiagency center tasked specifically with gathering and reviewing terrorist-related information. See § 52-47 (2009). The Department of State Police operates the fusion center, and it "shall collect, analyze, disseminate, and maintain such information to support local, state, and federal law-enforcement agencies, and other governmental agencies and private organizations in preventing, preparing for, responding to, and recovering from any possible or actual terrorist attack." Id.

¹⁶ Section 52-48(E).

¹⁷ Commonwealth v. Amerson, 281 Va. 414, 418, 706 S.E.2d 879, 882 (2011) (quoting Conger v. Barrett, 280 Va. 627, 630, 702 S.E.2d 117, 118 (2010)) (internal quotation marks omitted).

¹⁸ Kozmina v. Commonwealth, 281 Va. 347, 349, 706 S.E.2d 860, 862 (2011) (quoting Conyers v. Martial Arts World of Richmond, Inc., 273 Va. 96, 104, 639 S.E.2d 174, 178 (2007)).

¹⁹ See 2A NORMAN J. SINGER & J.D SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 47:23 (7th ed. 2007) (explaining maxim of statutory construction "expressio unius est exclusio alterius"). See also, e.g., 2008 Op. Va. Att'y Gen. 126, 127 and citations therein.

²⁰ Cnty. of Amherst v. Brockman, 224 Va. 391, 397 297 S.E.2d 805, 808 (1982).

²¹ Section 52-48(E) (emphasis added).

Col. W.S. Flaherty February 13, 2013 Page 5

to the identification and criminal activity of individuals or organizations that are reasonably suspected of involvement in criminal activity constitutes "criminal intelligence information." Information that has not been evaluated or determined to be so relevant does not meet the definition.

Accordingly, data collected by the fusion center through use of an LPR in the active manner, and specifically, the data that is evaluated and analyzed in real-time respecting suspected criminal activity, meets the definition of "criminal intelligence information." It thus is exempted from the scope of the Data Act.

Conversely, any data that may be collected in the passive manner by the fusion center through use of an LPR that is of unknown relevance and not intended for prompt evaluation and potential use respecting suspected criminal activity, is not "criminal intelligence information." It therefore is not exempted from the scope of the Data Act.

Therefore, in sum, I conclude that whether an LPR can be used to collect personal information depends on the manner in which the device is employed to obtain the data. If the data is collected in the active manner, including data that can be deemed "criminal intelligence information," such data can be collected, maintained and disseminated in accordance with law. On the other hand, LPR technology may not lawfully be used to collect personal information in the passive manner, including "the image of the place, the time, date and precise location [of a] license plate[.]"

Conclusion

Accordingly, it is my opinion that the Data Act does not preclude law enforcement agencies from maintaining, using and disseminating personal information collected by an LPR, provided such data specifically pertains to investigations and intelligence gathering relating to criminal activity. LPR data so collected is exempted from the Data Act's coverage. It further is my opinion that data collected by an LPR may be classified as "criminal intelligence information," and thereby exempted from the Data Act's coverage, if the data is collected by or on behalf of the Virginia Fusion Intelligence Center, is evaluated and determined to be relevant to criminal activity in accordance with, and is maintained in conformance with the criteria specified in § 52-48 of the Code of Virginia. Finally, it is my opinion that because the need for such data has not been "clearly established in advance", LPR data collected in the continuous, passive manner, that is not properly classified as "criminal intelligence information" and not otherwise relating directly to law enforcement investigations and intelligence gathering respecting criminal activity, is subject to the Data Act's strictures and prohibitions, and it may not lawfully be collected through use of LPR technology.

With kindest regards, I am

Very truly yours,

Kenneth T. Cuccinelli, II

Attorney General