COMMONWEALTH of VIRGINIA

Office of the Attorney General

Kenneth T. Cuccinelli, II
Attorney General

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

February 13, 2013

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 Act[1] 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.[7] 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.[8] 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 . . . ."[9] 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."[11]

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, "[t]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.[14] This exemption is found in another part of the Code, one that relates to the Virginia Fusion Intelligence Center ("the fusion center").[15] "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."[16] 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.[17] Where the language of a statute is unambiguous, the courts are bound by the plain meaning of that language.[18] Also, where a statute specifies certain things, the intention to exclude that which is not specified may be inferred,[19] and "[courts] may not add to a statute language which the legislature has chosen not to include."[20]

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 . . ."[21] 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).

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