S.155

Introduced by Senators Ashe, Benning, and Sears

Referred to Committee on Judiciary

Date: January 5, 2016

Subject: Privacy; medical records; drones; automated license plate readers

Statement of purpose of bill as introduced: This bill proposes a number of measures intended to enhance privacy protection. The bill includes the following provisions:

(1) The bill proposes to establish a private right of action for a person whose protected health care information is improperly disclosed.

(2) The bill proposes to establish regulations for the use of drones, also known as unmanned aerial vehicles. The bill proposes to permit a law enforcement agency to use a drone only if the agency obtains a warrant or if emergency circumstances exist.

(3) The bill proposes to restrict the use of automated license plate recognition (ALPR) systems, to address the confidentiality of data captured by ALPR systems, and to limit such data from being retained for more than 18 months unless certain exceptions apply.

An act relating to privacy protection

It is hereby enacted by the General Assembly of the State of Vermont:

* * * Protected Health Information * * *

Sec. 1. 18 V.S.A. chapter 42B is added to read:

CHAPTER 42B. HEALTH CARE PRIVACY

§ 1881. DISCLOSURE OF PROTECTED HEALTH INFORMATION PROHIBITED

(a) As used in this section:

(1) "Covered entity" shall have the same meaning as in 45 C.F.R. § 160.103.

(2) "Protected health information" shall have the same meaning as in 45 C.F.R. § 160.103.

(b) A covered entity shall not disclose protected health information unless the disclosure is permitted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

§ 1882. PRIVATE CAUSE OF ACTION

(a) A person whose protected health information is disclosed by a covered entity in violation of subsection 1881(b) of this title may bring an action in the Civil Division of the Superior Court for damages, injunctive relief, punitive damages, and reasonable costs and attorney's fees. The court may issue an award for the person's actual damages or $500.00 for a first violation or $1,000.00 for each subsequent violation, whichever is greater.

~~(b) This section shall not limit any other claims a person may have under applicable law.~~

Sec. 1. 18 V.S.A. chapter 42B is added to read:

CHAPTER 42B. HEALTH CARE PRIVACY

§ 1881. DISCLOSURE OF PROTECTED HEALTH INFORMATION PROHIBITED

(a) As used in this section:

(1) "Covered entity" shall have the same meaning as in 45 C.F.R. § 160.103.

(2) "Protected health information" shall have the same meaning as in 45 C.F.R. § 160.103.

(b) A covered entity shall not disclose protected health information unless the disclosure is permitted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

* * * Drones * * *

Sec. 2. 20 V.S.A. part 11 is added to read:

PART 11. DRONES

CHAPTER 205. DRONES

§ 4621. DEFINITIONS

As used in this chapter:

(1) "Drone" means a powered aerial vehicle that does not carry a human operator and is able to fly autonomously or to be piloted remotely.

(2) "Law enforcement agency" means:

(A) the Vermont State Police;

(B) a municipal police department;

(C) a sheriff's department;

(D) the Office of the Attorney General;

(E) a State's Attorney's office;

(F) the Capitol Police Department;

(G) the Department of Liquor Control;

(H) the Department of Fish and Wildlife;

(I) the Department of Motor Vehicles;

(J) a State investigator; or

(K) a person or entity acting on behalf of an agency listed in this subdivision (2).

§ 4622. LAW ENFORCEMENT USE OF DRONES

~~(a) Except as provided in subsection (b) of this section, a law enforcement agency shall not use a drone for any purpose or disclose or receive information acquired through the operation of a drone.~~

(a) Except as provided in subsection (b) of this section, a law enforcement agency shall not use a drone or information acquired through the use of a drone for the purpose of investigating, detecting, or prosecuting crime.

(b) A law enforcement agency may use a drone and may disclose or receive information acquired through the operation of a drone if the drone is operated under:

(1) a warrant obtained pursuant to Rule 41 of the Vermont Rules of Criminal Procedure; or

(2) emergency circumstances pursuant to section 4623 of this title.

(c)(1) When a drone is used pursuant to subsection (b) of this section, the drone shall be operated in a manner to collect data only on the target of the surveillance and to avoid data collection on any other person, home, or area.

(2) If a drone used pursuant to subsection (b) of this section collects data on any person, home, or area other than the target of the surveillance, the data:

(A) shall not be used, copied, or disclosed for any purpose; and

(B) shall be deleted as soon as possible and in no event later than 24 hours after the data were collected.

(3) Facial recognition or any other biometric matching technology shall not be used on any data that a drone collects on any person, home, or area other than the target of the surveillance.

(d) Information or evidence gathered in violation of this section shall be inadmissible in any judicial or administrative proceeding.

§ 4623. USE OF DRONES IN EMERGENCY SITUATIONS

(a) A law enforcement agency may use a drone and may disclose or receive information acquired through the operation of a drone if:

(1) an emergency situation exists in which it is reasonable to believe there is an imminent threat of death or serious bodily injury to any person; and

(2) the law enforcement agency obtains a search warrant for the use of the drone within 48 hours after the use commenced.

(b) If the court denies an application for a warrant filed pursuant to subdivision (a)(2) of this section:

(1) use of the drone shall cease immediately; and

(2) information or evidence gathered through use of the drone shall be destroyed and is inadmissible in any judicial or administrative proceeding.

(c) If a law enforcement agency using a drone in an emergency situation pursuant to this section obtains the information sought, the agency shall immediately cease use of the drone.

~~§ 4624. NONLAW ENFORCEMENT USE OF DRONES~~

(a) Any use of drones by any person other than a law enforcement agency shall comply with all Federal Aviation Administration requirements and guidelines.

(b) It is the intent of the General Assembly that any person who uses a model aircraft as defined in the Federal Aviation Administration Modernization and Reform Act of 2012 shall comply with the Academy of ~~Model Aeronautics National Model Aircraft Safety Code.~~

§ 4624. NONLAW ENFORCEMENT USE OF DRONES

(a) Any use of drones by any person other than a law enforcement agency shall comply with all applicable Federal Aviation Administration requirements and guidelines.

(b) It is the intent of the General Assembly that any person who uses a model aircraft as defined in the Federal Aviation Administration Modernization and Reform Act of 2012 shall operate the aircraft according to the guidelines of community-based organizations such as the Academy of Model Aeronautics National Model Aircraft Safety Code.

§ 4625. REPORTS

(a) On or before September 1 of each year, any law enforcement agency that has used a drone within the previous 12 months shall report the following information to the Department of Public Safety:

(1) The number of times the agency used a drone within the previous 12 months. For each use of a drone, the agency shall report the type of incident involved, the nature of the information collected, and the rationale for deployment of the drone.

(2) The number of criminal investigations aided and arrests made through use of information gained by the use of drones within the previous 12 months, including a description of how the drone aided each investigation or arrest.

(3) The number of times a drone collected data on any person, home, or area other than the target of the surveillance within the previous 12 months and the type of data collected in each instance.

(4) The cost of the agency's unmanned aerial vehicle program and the program's source of funding.

(b) On or before December 1 of each year that information is collected under subsection (a) of this section, the Department of Public Safety shall report the information to the House and Senate Committees on Judiciary and on Government Operations.

Sec. 3. 13 V.S.A. § 4018 is added to read:

§ 4018. DRONES

(a) No person shall equip a drone with a dangerous or deadly weapon or fire a projectile from a drone. A person who violates this section shall be imprisoned not more than one year or fined not more than $1,000.00, or both.

(b) As used in this section:

(1) "Drone" shall have the same meaning as in 20 V.S.A. § 4621.

(2) "Dangerous or deadly weapon" shall have the same meaning as in section 4016 of this title.

Sec. 4. REPORT; AGENCY OF TRANSPORTATION AVIATION PROGRAM

On or before December 15, 2016, the Aviation Program within the Agency of Transportation shall report to the Senate and House Committees on Judiciary any recommendations or proposals it determines are necessary for the regulation of drones pursuant to 20 V.S.A. § 4624.

** * * Vermont Electronic Communication Privacy Act * * **

Sec. 5. 13 V.S.A. chapter 232 is added to read:

CHAPTER 232. VERMONT ELECTRONIC COMMUNICATION PRIVACY ACT

§ 8101. DEFINITIONS

As used in this chapter:

(1) "Adverse result" means:

(A) danger to the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) serious jeopardy to an investigation or undue delay of a trial.

(2) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(3) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, a radio, electromagnetic, photoelectric, or photo-optical system.

(4) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including a service that acts as an intermediary in the transmission of electronic communications, or stores protected user information.

(5) "Electronic device" means a device that stores, generates, or transmits information in electronic form.

(6) "Government entity" means a department or agency of the State or a political subdivision thereof, or an individual acting for or on behalf of the State or a political subdivision thereof.

(7) "Law enforcement officer" means:

(A) a law enforcement officer certified at Level II or Level III pursuant to 20 V.S.A. § 2358;

(B) the Attorney General;

(C) an assistant attorney general;

(D) a State's Attorney; or

(E) a deputy State's attorney

(8) "Lawful user" means a person or entity who lawfully subscribes to or uses an electronic communication service, whether or not a fee is charged.

(9) "Protected user information" means electronic communication content, including the subject line of e-mails, cellular tower-based location data, GPS or GPS-derived location data, the contents of files entrusted by a user to an electronic communication service pursuant to a contractual relationship for the storage of the files whether or not a fee is charged, and data memorializing the content of information accessed or viewed by a user.

(10) "Service provider" means a person or entity offering an electronic communication service.

(11) "Specific consent" means consent provided directly to the government entity seeking information, including when the government entity

is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of a communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

(12) "Subscriber information" means the name, names of additional account users, account number, billing address, physical address, e-mail address, telephone number, payment method, record of services used, record of duration of service provided, and I.P. address kept by a service provider regarding a user or account.

§ 8102. LIMITATIONS ON COMPELLED PRODUCTION OF ELECTRONIC INFORMATION

(a) Except as provided in this section, a law enforcement officer shall not compel the production of or access to protected user information from a service provider.

(b) A law enforcement officer may compel the production of or access to protected user information from a service provider:

(1) pursuant to a warrant;

(2) pursuant to an existing, judicially recognized exception to the warrant requirement;

(3) with the specific consent of a lawful user of the electronic communication service;

(4) if a law enforcement officer, in good faith, believes that an emergency involving danger of death or serious bodily injury to any person requires access to the electronic device information without delay; or

(5) except where prohibited by State or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility, jail, or lock-up under the jurisdiction of the Department of Corrections, a sheriff, or a court to which inmates have access and the device is not in the possession of an individual and the device is not known or believed to be the possession of an authorized visitor.

(c) A law enforcement officer may compel the production of or access to information kept by a service provider other than protected user information:

(1) pursuant to a subpoena issued by a judicial officer, who shall issue the subpoena upon a finding that:

(A) there is reasonable cause to believe that an offense has been committed; and

(B) the information sought is relevant to the offense or appears reasonably calculated to lead to discovery of evidence of the alleged offense;

(2) pursuant to a subpoena issued by a grand jury;

(3) pursuant to a court order issued by a judicial officer upon a finding that the information sought is reasonably related to a pending investigation or pending case; or

(4) for any of the reasons listed in subdivisions (b)(2)–(4) of this section.

(d) A warrant issued for protected user information shall comply with the following requirements:

(1) The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought.

(2)(A) The warrant shall require that any information obtained through execution of the warrant that is unrelated to the warrant's objective not be subject to further review, use, or disclosure without a court order.

(B) A court shall issue an order for review, use, or disclosure of information obtained pursuant to subdivision (A) of this subdivision (2) if it finds there is probable cause to believe that:

(i) the information is relevant to an active investigation;

(ii) the information constitutes evidence of a criminal offense; or

(iii) review, use, or disclosure of the information is required by State or federal law.

(e) A warrant or subpoena directed to a service provider shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements of Rule 902(11) or 902(12) of the Vermont Rules of Evidence.

(f) A service provider may voluntarily disclose information other than protected user information when that disclosure is not otherwise prohibited by State or federal law.

(g) If a law enforcement officer receives information voluntarily provided pursuant to subsection (f) of this section, the officer shall destroy the information within 90 days unless any of the following circumstances apply:

(1) A law enforcement officer has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) A law enforcement officer obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist. The order shall authorize the retention of the information only for as long as:

(A) the conditions justifying the initial voluntary disclosure persist; or

(B) there is probable cause to believe that the information constitutes evidence of the commission of a crime.

(3) A law enforcement officer reasonably believes that the information relates to an investigation into child exploitation and the information is retained as part of a multiagency database used in the investigation of similar offenses and related crimes.

(h) If a law enforcement officer obtains electronic information without a warrant under subdivision (b)(4) of this section because of an emergency involving danger of death or serious bodily injury to a person that requires access to the electronic information without delay, the officer shall, within five days after obtaining the information, apply for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures. The application or motion shall set forth the facts giving rise to the emergency and shall, if applicable, include a request supported by a sworn affidavit for an order delaying notification under subdivision 8103(b)(1) of this section. The court shall promptly rule on the application or motion. If the court finds that the facts did not give rise to an emergency or denies the motion or application on any other ground, the court shall order the immediate destruction of all information obtained, and immediate notification pursuant to subsection 8103(a) if this title if it has not already been provided.

(i) This section does not limit the existing authority of a law enforcement officer to use legal process to do any of the following:

(1) require an originator, addressee, or intended recipient of an electronic communication to disclose any protected user information associated with that communication;

(2) require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties to disclose protected user information associated with an

electronic communication to or from an officer, director, employee, or agent of the entity; or

(3) require a service provider to provide subscriber information.

(j) A service provider shall not be subject to civil or criminal liability for producing or providing access to information in good faith reliance on the provisions of this section. This subsection shall not apply to gross negligence, recklessness, or intentional misconduct by the service provider.

§ 8103. NOTICE TO USER OR SUBSCRIBER

(a) Except as otherwise provided in this section, a law enforcement officer who executes a warrant or obtains electronic information in an emergency pursuant to subdivision 8102(b)(4) of this section shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request a notice that informs the recipient that information about the recipient has been compelled or requested, and, if there was an emergency request, states with reasonable specificity the nature of the government action relative to which the information is sought. The notice shall include a copy of the warrant if a warrant was obtained. The notice shall be served, mailed, or delivered by reliable electronic means contemporaneously with the execution of the warrant, or, in the case of an emergency, within three days after obtaining the electronic information.

(b)(1) When a warrant is sought or electronic information is obtained in an emergency under subdivision 8102(b)(4) of this title, the law enforcement officer may submit a request supported by a sworn affidavit for an order delaying the notification required by subsection (a) of this section and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if it determines that there is reason to believe that notification may have an adverse result. The delay shall not exceed the period of time for which the court finds there is reason to believe that the notification may have the adverse result, and in no event shall the delay exceed 90 days.

(2) The court may grant additional extensions of the delay for periods of up to 90 days each on the same grounds as provided for in subdivision (1) of this subsection.

(3) When the delayed notification period expires, a law enforcement officer shall serve upon, or deliver to by registered or first-class mail, electronic mail, or reliable electronic means the order for delayed notification, the identified targets of the warrant:

(A) a document that includes the information described in subsection (a) of this section; and

(B) a copy of all electronic information obtained or a summary of that information, including, at a minimum:

(i) the number and types of records disclosed;

(ii) the date and time when the earliest and latest records were created; and

(iii) a copy of the motion seeking delayed notification.

(c) If there is no identified target of a warrant or emergency request at the time of its issuance, the government entity shall submit to the Department of Public Safety within three days of the execution of the warrant or issuance of the request all of the information required by subsection (a) of this section. If an order delaying notice is issued pursuant to subsection (b) of this section, the law enforcement officer shall submit to the Department upon the expiration of the delayed notification period all of the information required in subdivision (b)(3) of this section. The Department shall publish all reports required by this subsection on its Internet website within 90 days of receipt. The Department shall redact names and other identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

(e) For purposes of this chapter, a warrant served upon a service provider is deemed to have been executed no later than five days after the information or data compelled by the warrant has been produced by the service provider to a law enforcement officer.

§ 8104. EXCLUSIVE REMEDIES FOR A VIOLATION OF THIS CHAPTER

(a) A defendant in a trial, hearing, or proceeding may move to suppress electronic information obtained or retained in violation of the U.S. Constitution, the Vermont Constitution, or this chapter.

(b) A defendant in a trial, hearing, or proceeding shall not move to suppress electronic information on the ground that Vermont lacks personal jurisdiction over a service provider, or on the ground that the constitutional or statutory privacy rights of an individual other than the defendant were violated.

(c) A service provider who receives a subpoena issued pursuant to this chapter may file a motion to quash the subpoena. The motion shall be filed in

the court that issued the subpoena before the expiration of the time period for production of the information. The court shall hear and decide the motion as soon as practicable. Consent to additional time to comply with process under section 806 of this title does not extend the date by which a service provider shall seek relief under this subsection.

§ 8105. EXECUTION OF WARRANT FOR INFORMATION KEPT BY SERVICE PROVIDER

A warrant issued under this chapter may be addressed to any Vermont law enforcement officer. The officer shall serve the warrant upon the service provider, the service provider's registered agent, or, if the service provider has no registered agent in the State, upon the Office of Secretary of State in accordance with 12 V.S.A. §§ 851–858. If the service provider consents, the warrant may be served via U.S. mail, courier service, express delivery service, facsimile, electronic mail, an Internet-based portal maintained by the service provider, or other reliable electronic means. The physical presence of the law enforcement officer at the place of service or at the service provider's repository of data shall not be required.

§ 8106. SERVICE PROVIDER'S RESPONSE TO WARRANT

The service provider shall produce the items listed in the warrant within 20 days in a manner and format that permits them to be searched by the law enforcement officer. The court may, for good cause shown, shorten or lengthen the 20-day deadline. This section shall not be construed to limit the authority of a law enforcement officer under existing law to search personally for and locate items or data on the premises of a Vermont service provider.

§ 8107. CRIMINAL PROCESS ISSUED BY VERMONT COURT; RECIPROCITY

(a) Criminal process, including subpoenas, search warrants, and other court orders issued pursuant to this chapter, may be served and executed upon any service provider within or outside the State, provided the service provider has contact with Vermont sufficient to support personal jurisdiction over it by this State. Notwithstanding any other provision in this chapter, only a service provider may challenge legal process, or the admissibility of evidence obtained pursuant to it, on the ground that Vermont lacks personal jurisdiction over it.

(b) This section shall not be construed to limit the authority of a court to issue criminal process under any other provision of law.

(c) A service provider incorporated, domiciled, or with a principal place of business in Vermont that has been properly served with criminal process issued by a court of competent jurisdiction in another state, commonwealth,

territory, or political subdivision thereof shall comply with the legal process as though it had been issued by a court of competent jurisdiction in this State.

§ 8108. REAL TIME INTERCEPTION OF INFORMATION PROHIBITED

A law enforcement officer shall not use a device which via radio or other electromagnetic wireless signal intercepts in real time from a user's device a transmission of communication content, real time cellular tower-derived location information, or real time GPS-derived location information, except for purposes of locating and apprehending a fugitive for whom an arrest warrant has been issued. This section shall not be construed to prevent a law enforcement officer from obtaining information from an electronic communication service as otherwise permitted by law.

* * * Automated License Plate Recognition Systems * * *

Sec. ~~4~~ *6*. 23 V.S.A. § 1607a is added to read:

§ 1607a. AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS

(a) Definitions. As used in this section and section 1608a of this title:

(1) "Automated license plate recognition system" or "ALPR system" means a system of one or more mobile or fixed high-speed cameras combined with computer algorithms that convert images of license plates into computer-readable files of license plate numbers.

(2) "Captured plate data" means:

(A) the data captured by an ALPR system, including a photograph of a license plate, GPS coordinates of the location of a license plate, and the date and time that an ALPR system captured data relating to a license plate; and

(B) the files of license plate numbers derived from images of license plates.

(3) "Department" means the Department of Public Safety.

(4) "Law enforcement officer" means a State Police officer, municipal police officer, motor vehicle inspector, Capitol Police officer, constable, sheriff, or deputy sheriff who is certified by the Vermont Criminal Justice Training Council as a Level II or Level III law enforcement officer under 20 V.S.A. § 2358.

(5) "Legitimate law enforcement purpose" means:

(A) detection, investigation, analysis, or enforcement of a crime, traffic violation, or parking violation;

(B) defending against a pending or reasonably anticipated charge or complaint of a crime, traffic violation, or parking violation;

(C) operation of AMBER alerts; or

(D) missing or endangered person searches.

(6) "Vermont law enforcement agency" means:

(A) the Department of Public Safety;

(B) a municipal police department;

(C) a sheriff's department;

(D) the Office of the Attorney General;

(E) a State's Attorney's office;

(F) the Capitol Police Department;

(G) the Department of Motor Vehicles.

(7) "Warrant" means a warrant issued pursuant to Rule 41 of the Vermont or Federal Rules of Criminal Procedure.

(b) Restrictions on use of ALPR systems; ALPR database content.

(1) A person shall not operate an ALPR system in Vermont unless he or she is a law enforcement officer and operates the system for a legitimate law enforcement purpose. A law enforcement officer shall not operate an ALPR system in Vermont unless:

(A) the officer is certified in ALPR operation by the Vermont Criminal Justice Training Council; and

(B) the system automatically transfers captured plate data to the statewide ALPR server maintained by the Department and captured plate data are automatically deleted from the system after the data's transfer to the Department.

(2) A Department supervisor must approve the entry of any data onto the statewide ALPR server other than data collected by an ALPR system itself, and any such entry shall be for a legitimate law enforcement purpose.

(c) Confidentiality of captured plate data; exceptions.

(1) Except as provided in this subsection, captured plate data are exempt from public inspection and copying under the Public Records Act and shall be kept confidential. Captured plate data shall not be subject to subpoena or discovery, or be admissible in evidence, in any private civil action.

(2)(A) Upon request, the Department may disclose captured plate data lawfully retained under this section for a legitimate law enforcement purpose. A receiving person may use the data or further disclose it, but only for a legitimate law enforcement purpose.

(B) Any requests for captured plate data from the Department under this subdivision (2) shall be in writing and include the name of the requester and, if applicable, the law enforcement agency the requester is employed by and the law enforcement agency's Originating Agency Identifier number. The request shall describe the legitimate law enforcement purpose for which the data are to be used. The Department shall retain all requests and record in writing the outcome of the request and any information that was provided to the requester or, if applicable, its reasons for denying or not fulfilling the request. The Department shall retain the information described in this subdivision (c)(2)(B) for at least three years.

(3) The Department shall not release captured plate data to a person unless the person has accepted the terms of a user agreement with the Department. The user agreement shall specify the confidentiality, permitted uses, and authorized retention periods of the data in accordance with the provisions of this section.

(d) Limitation on retention of captured plate data; extensions, exception.

(1) A person shall not retain captured plate data for more than 18 months after the date of its creation unless:

(A) this period is extended under a warrant or pursuant to section 1608a of this title; or

(B) the plate data is relevant to the defense of a pending or reasonably anticipated charge or complaint.

(2) Except for captured plate data described in subdivision (1)(B) of this subsection, captured plate data shall be destroyed upon the expiration of the 18-month period, plus any authorized extension of this period.

(e) Applicability to data received from other jurisdictions. This section shall apply to captured plate data received from outside Vermont, whether from a public or private person. Such data shall be retained and used consistent with the requirements of this section and of the sending person.

(f) Special provisions for commercial motor vehicle enforcement. With respect to the use of ALPRs for commercial motor vehicle screening, inspection, and compliance activities pursuant to Federal Motor Carrier Safety Regulations:

(1) Notwithstanding subdivisions (b)(1)(B) and (b)(2) of this section:

(A) Captured plate data are not required to be automatically transferred to the Department of Public Safety. However, data must be transferred from an ALPR system to a centralized ALPR database designated

by the Department of Motor Vehicles and deleted from individual ALPR units after the transfer.

(B) A Department of Motor Vehicle supervisor must approve the entry of data onto the centralized database.

(2) The Department of Motor Vehicles shall have the same authority and responsibilities as the Department of Public Safety as specified in subsection (c) of this section.

(g) Penalties.

(1) A person who knowingly uses an ALPR system or captured plate data in violation of this section or who knowingly violates the confidentiality provisions of this section shall be fined not more than $1,000.00 or imprisoned not more than two years, or both.

(2) A person who knowingly retains captured plate data beyond the time limits established under this section and section 1608a of this title shall be fined not more than $500.00.

(h) Oversight. The Department, in consultation with the Department of Motor Vehicles, shall establish a review process to ensure that information obtained through the use of ALPR systems is used only for the purposes permitted under this section. The Department shall report the results of this review annually on or before January 15 to the Senate and House Committees on Judiciary. The report shall contain the following information based on prior

calendar year data in connection with the statewide ALPR database and, if applicable, for any separate ALPR database that may be established in connection with commercial motor vehicle enforcement:

(1) the total number of ALPR units being operated in the State and the number of units submitting data;

(2) the total number of ALPR readings that each agency submitted to the database;

(3) the 12-month cumulative number of ALPR readings retained on the database for more than 18 months;

(4) the total number of requests made for ALPR data;

(5) the total number of requests that resulted in release of information;

(6) the total number of out-of-state requests; and

(7) the total number of out-of-state requests that resulted in release of information.

(i) Rulemaking authority. The Department may adopt rules to implement this section.

Sec. ~~5~~ 7. 23 V.S.A. § 1608a is added to read:

§ 1608a. PRESERVATION OF DATA

(a) Preservation request.

(1) An out-of-state or Vermont law enforcement agency or a person against whom a charge or complaint is pending or is reasonably anticipated to

be brought or his or her representative may apply to the Criminal Division of the Superior Court for an extension of up to 90 days of the 18-month retention period established under subsection 1607a(d) of this title if the agency or person offers specific and articulable facts showing that there are reasonable grounds to believe that the captured plate data are relevant and material to an ongoing criminal or missing persons investigation or to a pending court or Judicial Bureau traffic proceeding. Requests for additional 90-day extensions or for extensions of longer duration may be made to the court subject to the same standards applicable to an initial extension request under this subdivision.

(2) A person making a preservation request under this section shall submit an affidavit stating:

(A) the particular camera or cameras for which captured plate data must be preserved or the particular license plate for which captured plate data must be preserved; and

(B) the date or dates and time frames for which captured plate data must be preserved.

(b) If a request for a preservation order is denied, the captured plate data shall be destroyed upon the final denial of the request on appeal or upon the expiration or waiver of appeal rights, unless the data are required to be preserved under a warrant.

* * * Effective Date * * *

~~Sec. 6. EFFECTIVE DATE~~

~~This act shall take effect on July 1, 2016.~~

Sec. 8. EFFECTIVE DATES

(a) Secs. 6, 7, and this section shall take effect on July 1, 2016.

(b) Secs. 1, 2, 3, 4, and 5 shall take effect on October 1, 2016.