S.155

An act relating to privacy protection and a code of administrative rules

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).

* * * 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 (c) 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)(1) A law enforcement agency shall not use a drone to gather or retain data on private citizens peacefully exercising their constitutional rights of free speech and assembly.

(2) This subsection shall not be construed to prohibit a law enforcement agency from using a drone:

(A) for observational, public safety purposes that do not involve gathering or retaining data; or

(B) pursuant to a warrant obtained under Rule 41 of the Vermont Rules of Criminal Procedure.

(c) 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:

(1) for a purpose other than the investigation, detection, or prosecution of crime, including search and rescue operations and aerial photography for the assessment of accidents, forest fires and other fire scenes, flood stages, and storm damage; or

(2) pursuant to:

(A) a warrant obtained under Rule 41 of the Vermont Rules of Criminal Procedure; or

(B) a judicially recognized exception to the warrant requirement.

(d)(1) When a drone is used pursuant to subsection (c) of this section, the drone shall be operated in a manner intended to collect data only on the target

of the surveillance and to avoid data collection on any other person, home, or area.

(2) 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.

(3)(A) If a law enforcement agency uses a drone in exigent circumstances pursuant to subdivision (c)(2)(B) of this section, the agency shall obtain 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) of this subdivision (d)(3):

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

(ii) information or evidence gathered through use of the drone shall be destroyed.

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

§ 4623. USE OF DRONES; FEDERAL AVIATION ADMINISTRATION REQUIREMENTS

(a) Any use of drones by any person, including 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.

§ 4624. 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 drone 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. § 4623.

* * * 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) "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.

(3) "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.

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

(5) "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.

(6) "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

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

(8) "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, data memorializing the content of information accessed or viewed by a user, and any other data for which a reasonable expectation of privacy exists.

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

(10) "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.

(11) "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, and record of duration of service provided or 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 a 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 in 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)(1)–(3) 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 to the identified targets of the warrant:

(A) the order for delayed notification;

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

(C) 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 8106 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

(a) The service provider shall produce the items listed in the warrant within 30 days unless the court orders a shorter period for good cause shown, in which case the court may order the service provider to produce the items listed

in the warrant within 72 hours. The items shall be produced in a manner and format that permits them to be searched by the law enforcement officer.

(b) 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.

(c) As used in this section, "good cause" includes an investigation into a homicide, kidnapping, unlawful restraint, custodial interference, felony punishable by life imprisonment, or offense related to child exploitation.

§ 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. 6. EXTENSION OF SUNSET

2013 Acts and Resolves No. 69, Sec. 3, as amended by 2015 Acts and Resolves No. 32, Sec. 1, is further amended to read:

Sec. 3. EFFECTIVE DATE AND SUNSET

* * *

(b) Secs. 1–2 of this act, 23 V.S.A. §§ 1607 and 1608, shall be repealed on July 1, ~~2016~~ 2018.

Sec. 7. ANALYSIS OF ALPR SYSTEM-RELATED COSTS AND BENEFITS

(a) On or before January 15, 2017, the Department of Public Safety, in consultation with the Joint Fiscal Office, shall:

(1) Estimate the total annualized fixed and variable costs associated with all automated license plate recognition (ALPR) systems used by law enforcement officers in Vermont, including capital, operating, maintenance, personnel, training, and other costs. The estimate shall include a breakdown of costs by category.

(2) Estimate the total annualized fixed and variable costs associated with any planned increase in the number of ALPR systems used by law enforcement officers in Vermont and with any planned increase in the intensity of use of existing ALPR systems, including capital, operating, maintenance, personnel, training, and other costs. The estimate shall include a breakdown of costs by category.

(3) Conduct a cost-benefit analysis of the existing and planned use of ALPR systems in Vermont, and an analysis of how these costs and benefits compare with other enforcement tools that require investment of Department resources.

(b) On or before January 15, 2017, the Department of Public Safety shall submit a written report to the House and Senate Committees on Judiciary and

on Transportation of the estimates and analysis required under subsection (a) of this section.

(c) If the Department of Motor Vehicles establishes or designates an independent server to store data captured by ALPRs before January 15, 2017, it shall conduct the analysis required under subsection (a) of this section in consultation with the Joint Fiscal Office and submit a report in accordance with subsection (b) of this section.

Sec. 8. 23 V.S.A. § 1607 is amended to read:

§ 1607. AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS

(a) Definitions. As used in this section:

(1) "Active data" is distinct from historical data as defined in subdivision (3) of this subsection and means data uploaded to individual automated license plate recognition system units before operation as well as data gathered during the operation of an ALPR system. Any data collected by an ALPR system in accordance with this section shall be considered collected for a legitimate law enforcement purpose.

(2) "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 to convert images of registration plates into computer-readable data.

(3) "Historical data" means any data collected by an ALPR system and stored on the statewide ALPR server operated by the Vermont Justice Information Sharing System of the Department of Public Safety. Any data collected by an ALPR system in accordance with this section shall be considered collected for a legitimate law enforcement purpose.

(4) "Law enforcement officer" means a State Police officer, municipal police officer, motor vehicle inspector, Capitol Police officer, constable, sheriff, or deputy sheriff certified by the Vermont Criminal Justice Training Council as ~~having satisfactorily completed the approved training programs required to meet the minimum training standards applicable to that person~~ a level II or level III law enforcement officer under 20 V.S.A. § 2358.

(5) "Legitimate law enforcement purpose" applies to access to active or historical data, and means investigation, detection, analysis, or enforcement of a crime~~, traffic violation, or parking violation~~ or of a commercial motor vehicle violation or a person's defense against a charge of a crime or commercial motor vehicle violation, or operation of AMBER alerts or missing or endangered person searches.

(6) "Vermont ~~Information and Analysis~~ Intelligence Center ~~Analyst~~ analyst" means any sworn or civilian employee who through his or her employment with the Vermont ~~Information and Analysis~~ Intelligence Center

~~(VTIAC)~~ (VIC) has access to secure databases that support law enforcement investigations.

(b) Operation. A Vermont law enforcement officer shall be certified in ALPR operation by the Vermont Criminal Justice Training Council in order to operate an ALPR system.

(c) ALPR use and data access; confidentiality.

(1)(A) Deployment of ALPR equipment by Vermont law enforcement agencies is intended to provide access to law enforcement reports of wanted or stolen vehicles and wanted persons and to further other legitimate law enforcement purposes. Use of ALPR systems by law enforcement officers and access to active data are restricted to legitimate law enforcement purposes.

(B) Active ~~ALPR~~ data may be accessed by a law enforcement officer operating the ALPR system only if he or she has a legitimate law enforcement purpose for the data. Entry of any data into the system other than data collected by the ALPR system itself must be approved by a supervisor and shall have a legitimate law enforcement purpose.

(C)(i) Requests to ~~review~~ access active data shall be in writing and include the name of the requester, the law enforcement agency the requester is employed by, if any, and the law enforcement agency's Originating Agency Identifier (ORI) number. ~~The~~ To be approved, the request ~~shall describe the legitimate law enforcement purpose~~ must provide specific and articulable facts

showing that there are reasonable grounds to believe that the data are relevant and material to an ongoing criminal, missing person, or commercial motor vehicle investigation or enforcement action. The written request and the outcome of the request shall be transmitted to ~~VTIAC~~ VIC and retained by ~~VTIAC~~ VIC for not less than three years.

(ii) In each department operating an ALPR system, access to active data shall be limited to designated personnel who have been provided account access by the department to conduct authorized ALPR stored data queries. Access to active data shall be restricted to data collected within the past seven days.

(2)(A) A ~~VTIAC~~ VIC analyst shall transmit historical data only to a Vermont or out-of-state law enforcement officer or person who has a legitimate law enforcement purpose for the data. A law enforcement officer or other person to whom historical data are transmitted may use such data only for a legitimate law enforcement purpose. Entry of any data onto the statewide ALPR server other than data collected by an ALPR system itself must be approved by a supervisor and shall have a legitimate law enforcement purpose.

(B) Requests for historical data within six months of the date of the data's creation, whether from Vermont or out-of-state law enforcement officers or other persons, shall be made in writing to ~~an analyst at VTIAC~~ a VIC analyst. The request shall include the name of the requester, the law

enforcement agency the requester is employed by, if any, and the law enforcement agency's ORI number. ~~The~~ To be approved, the request ~~shall describe the legitimate law enforcement purpose~~ must provide specific and articulable facts showing that there are reasonable grounds to believe that the data are relevant and material to an ongoing criminal, missing person, or commercial motor vehicle investigation or enforcement action. ~~VTIAC~~ VIC shall retain all requests and shall record in writing the outcome of the request and any information that was provided to the requester or, if applicable, why a request was denied or not fulfilled. ~~VTIAC~~ VIC shall retain the information described in this subdivision (c)(2)(B) for no fewer than three years.

(C) After six months from the date of its creation, VIC may only disclose historical data:

(i) pursuant to a warrant if the data are not sought in connection with a pending criminal charge; or

(ii) to the prosecution or the defense in connection with a pending criminal charge and pursuant to a court order issued upon a finding that the data are reasonably likely to be relevant to the criminal matter.

(3) Active data and historical data shall not be subject to subpoena or discovery, or be admissible in evidence, in any private civil action.

(4) Notwithstanding any contrary provisions of subdivision (2) of this subsection, in connection with commercial motor vehicle screening,

inspection, and compliance activities to enforce the Federal Motor Carrier Safety Regulations, the Department of Motor Vehicles (DMV):

(A) may maintain or designate a server for the storage of historical data that is separate from the statewide server;

(B) may designate a DMV employee to carry out the same responsibilities as a VIC analyst and a supervisor as specified in subdivision (2) of this subsection; and

(C) shall have the same duties as the VIC with respect to the retention of requests for historical data.

(d) Retention.

(1) Any ALPR information gathered by a Vermont law enforcement agency shall be sent to the Department of Public Safety to be retained pursuant to the requirements of subdivision (2) of this subsection. The Department of Public Safety shall maintain the ALPR storage system for Vermont law enforcement agencies.

(2) Except as provided in this subsection and section 1608 of this title, information gathered by a law enforcement officer through use of an ALPR system shall only be retained for 18 months after the date it was obtained. When the permitted 18-month period for retention of the information has expired, the Department of Public Safety and any local law enforcement agency with custody of the information shall destroy it and cause to have

destroyed any copies or backups made of the original data. Data may be retained beyond the 18-month period pursuant to a preservation request made or disclosure order issued under Section 1608 of this title or pursuant to a warrant issued under Rule 41 of the Vermont or Federal Rules of Criminal Procedure.

(e) Oversight; rulemaking.

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

(A) the total number of ALPR units being operated in the State and the number of units submitting data to the statewide ALPR database;

(B) the ~~total~~ number of ALPR readings each agency submitted, and the total number of all such readings submitted, to the statewide ALPR database;

(C) the 18-month cumulative number of ALPR readings being housed on the statewide ALPR database as of the end of the calendar year;

(D) the total number of requests made to ~~VTIAC~~ VIC for ~~ALPR~~ historical data~~;~~

~~(E)~~, the average age of the data requested, and the ~~total~~ number of these requests that resulted in release of information from the statewide ALPR database;

~~(F)~~(E) the total number of out-of-state requests~~; and~~

~~(G)~~ to VIC for historical data, the average age of the data requested, and the ~~total~~ number of out-of-state requests that resulted in release of information from the statewide ALPR database;

(F) the total number of alerts generated on ALPR systems operated by law enforcement officers in the State by a match between an ALPR reading and a plate number on an alert database and the number of these alerts that resulted in an enforcement action;

(G) the total number of criminal, missing person, and commercial motor vehicle investigations and enforcement actions to which active data contributed, and a summary of the nature of these investigations and enforcement actions;

(H) the total number of criminal, missing person, and commercial motor vehicle investigations and enforcement actions to which historical data contributed, and a summary of the nature of these investigations and enforcement actions; and

(I) the total annualized fixed and variable costs associated with all ALPR systems used by Vermont law enforcement agencies and an estimate of the total of such costs per unit.

(2) ~~The~~ Before January 1, 2018, the Department of Public Safety ~~may~~ shall adopt rules to implement this section.

Sec. 9. 23 V.S.A. § 1608 is amended to read:

§ 1608. PRESERVATION OF DATA

(a) Preservation request.

(1) A law enforcement agency or the Department of Motor Vehicles or other person with a legitimate law enforcement purpose 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 subdivision 1607(d)(2) of this title if the agency or Department 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 proceeding involving enforcement of a crime or of a commercial motor vehicle violation. Requests for additional 90-day extensions or for longer periods may be made to the Superior Court subject to the same standards applicable to an initial extension request under this subdivision.

(2) A governmental entity 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) Captured plate data shall be destroyed on the schedule specified in section 1607 of this title if the preservation request is denied or 14 days after the denial, whichever is later.

* * * Information Related to Use of Ignition Interlock Devices * * *

Sec. 10. 23 V.S.A. § 1213 is amended to read:

§ 1213. IGNITION INTERLOCK RESTRICTED DRIVER'S LICENSE; PENALTIES

* * *

(m)(1) Images and other individually identifiable information in the custody of a public agency related to the use of an ignition interlock device is exempt from public inspection and copying under the Public Records Act and shall not be disclosed except:

(A) pursuant to a warrant;

(B) 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 information without delay; or

(C) in connection with enforcement proceedings under this section or rules adopted pursuant to this section.

(2) Images or information disclosed in violation of this subsection shall be inadmissible in any judicial or administrative proceeding.

* * * Administrative Procedure Act; Code of Administrative Rules * * *

Sec. 11. 3 V.S.A. § 847 is amended to read:

§ 847. AVAILABILITY OF ADOPTED RULES; RULES BY SECRETARY OF STATE

(a) The Secretary of State shall keep open to public inspection a permanent register of rules. The Secretary also shall publish a code of administrative rules that contains the rules adopted under this chapter. The requirement to publish a code shall be considered satisfied if a commercial publisher offers such a code in print at a competitive price and at no charge online.

(b) The Secretary of State shall publish not less than quarterly a bulletin setting forth the text of all rules filed since the immediately preceding publication and any objections filed under subsection 842(b) or 844(e) of this title. The provisions of 2 V.S.A. § 20(d) (expiration of required reports) shall not apply to the report to be made under this subsection.

(c) The bulletin may omit any rule if either:

(1) a commercial publisher offers a comparable publication at a competitive price; or

(2) all three of the following apply:

(A) its publication would be unduly cumbersome or expensive; and

(B) the rule is made available on application to the adopting agency; and

(C) the bulletin contains a notice stating the general subject matter of the omitted rule and stating how a copy of the rule and any objection filed under subsection 842(b) or 844(e) of this title may be obtained.

(d) Bulletins shall be made available upon request to agencies and officials of this State free of charge and to other persons at prices fixed by the Secretary of State to cover mailing and publication costs.

(e) The Secretary of State shall adopt rules for the effective administration of this chapter. These rules shall be applicable to every agency and shall include ~~but not be limited to~~ uniform procedural requirements, style, appropriate forms, and a system for compiling and indexing rules.

Sec. 12. 3 V.S.A. § 848 is amended to read:

§ 848. RULES REPEAL; OPERATION OF LAW

(a) A rule shall be repealed without formal proceedings under this chapter if:

(1) the agency ~~which~~ that adopted the rule is abolished and its authority, specifically including its authority to implement its existing rules, has not been transferred to another agency~~,~~; or

(2) a court of competent jurisdiction has declared the rule to be invalid~~,~~; or

(3) the statutory authority for the rule, as stated by the agency under subdivision 838(b)(4) of this title, is repealed by the General Assembly or declared invalid by a court of competent jurisdiction.

(b) When a rule is repealed by operation of law under this section, the Secretary of State shall delete the rule from the published code of administrative rules.

(c)(1) On July 1, 2018, a rule shall be repealed without formal proceedings under this chapter if:

(A) as of July 1, 2016, the rule was in effect but not published in the code of administrative rules; and

(B) the rule is not published in such code before July 1, 2018.

(2) An agency seeking to publish a rule described in subdivision (1) of this subsection may submit a digital copy of the rule to the Secretary of State with proof acceptable to the Secretary that as of July 1, 2016 the rule was adopted and in effect under this chapter and the digital copy consists of the text of such rule without change.

(d) If the statutory authority for a rule, as stated by the agency under subdivision 838(b)(4), is amended by the General Assembly, the agency shall review the rule and make a determination whether such statutory amendment repeals the authority upon which the rule is based, and shall, within 60 days of the effective date of the statutory amendment, inform in writing the Secretary of State and the Legislative Committee on Administrative Rules whether repeal or revision of the rule is required by the statutory amendment.

* * * Effective Dates * * *

Sec. 13. EFFECTIVE DATES

(a) This section and Secs. 6–7 shall take effect on passage.

(b) Secs. 8–12 shall take effect on July 1, 2016, except that in Sec. 8, 23 V.S.A. § 1607(e)(1) (oversight, reporting) shall take effect on January 16, 2017.

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