

1 TO THE HOUSE OF REPRESENTATIVES:

2 The Committee on Judiciary to which was referred Senate Bill No. 155
3 entitled “An act relating to privacy protection” respectfully reports that it has
4 considered the same and recommends that the House propose to the Senate that
5 the bill be amended by striking out all after the enacting clause and inserting in
6 lieu thereof the following:

7 * * * Protected Health Information * * *

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

9 CHAPTER 42B. HEALTH CARE PRIVACY

10 § 1881. DISCLOSURE OF PROTECTED HEALTH INFORMATION

11 PROHIBITED

12 (a) As used in this section:

13 (1) “Covered entity” shall have the same meaning as in 45 C.F.R.

14 § 160.103.

15 (2) “Protected health information” shall have the same meaning as in

16 45 C.F.R. § 160.103.

17 (b) A covered entity shall not disclose protected health information unless

18 the disclosure is permitted under the Health Insurance Portability and

19 Accountability Act of 1996 (HIPAA).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

* * * 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).

1 § 4622. LAW ENFORCEMENT USE OF DRONES

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

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

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

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

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

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

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

1 (2) pursuant to:

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

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

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

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

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

14 § 4623. USE OF DRONES; FEDERAL AVIATION ADMINISTRATION
15 REQUIREMENTS

16 (a) Any use of drones by any person, including a law enforcement agency,
17 shall comply with all applicable Federal Aviation Administration requirements
18 and guidelines.

19 (b) It is the intent of the General Assembly that any person who uses a
20 model aircraft as defined in the Federal Aviation Administration
21 Modernization and Reform Act of 2012 shall operate the aircraft according to

1 the guidelines of community-based organizations such as the Academy of
2 Model Aeronautics National Model Aircraft Safety Code.

3 § 4624. REPORTS

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

7 (1) The number of times the agency used a drone within the previous
8 12 months. For each use of a drone, the agency shall report the type of
9 incident involved, the nature of the information collected, and the rationale for
10 deployment of the drone.

11 (2) The number of criminal investigations aided and arrests made
12 through use of information gained by the use of drones within the previous
13 12 months, including a description of how the drone aided each investigation
14 or arrest.

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

18 (4) The cost of the agency's drone program and the program's source of
19 funding.

20 (b) On or before December 1 of each year that information is collected
21 under subsection (a) of this section, the Department of Public Safety shall

1 report the information to the House and Senate Committees on Judiciary and
2 on Government Operations.

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

4 § 4018. DRONES

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

8 (b) As used in this section:

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

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

12 Sec. 4. REPORT; AGENCY OF TRANSPORTATION AVIATION
13 PROGRAM

14 On or before December 15, 2016, the Aviation Program within the Agency
15 of Transportation shall report to the Senate and House Committees on
16 Judiciary any recommendations or proposals it determines are necessary for
17 the regulation of drones pursuant to 20 V.S.A. § 4623.

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

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

3 CHAPTER 232. VERMONT ELECTRONIC COMMUNICATION

4 PRIVACY ACT

5 § 8101. DEFINITIONS

6 As used in this chapter:

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

10 (2) “Electronic communication service” means a service that provides to
11 its subscribers or users the ability to send or receive electronic
12 communications, including a service that acts as an intermediary in the
13 transmission of electronic communications, or stores protected user
14 information.

15 (3) “Electronic device” means a device that stores, generates, or
16 transmits information in electronic form.

17 (4) “Government entity” means a department or agency of the State or a
18 political subdivision thereof, or an individual acting for or on behalf of the
19 State or a political subdivision thereof.

1 (5) “Law enforcement officer” means:

2 (A) a law enforcement officer certified at Level II or Level III

3 pursuant to 20 V.S.A. § 2358;

4 (B) the Attorney General;

5 (C) an assistant attorney general;

6 (D) a State’s Attorney; or

7 (E) a deputy State’s attorney

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

10 (7) “Protected user information” means electronic communication
11 content, including the subject line of e-mails, cellular tower-based location
12 data, GPS or GPS-derived location data, the contents of files entrusted by a
13 user to an electronic communication service pursuant to a contractual
14 relationship for the storage of the files whether or not a fee is charged, data
15 memorializing the content of information accessed or viewed by a user, and
16 any other data for which a reasonable expectation of privacy exists.

17 (8) “Service provider” means a person or entity offering an electronic
18 communication service.

19 (9) “Specific consent” means consent provided directly to the
20 government entity seeking information, including when the government entity
21 is the addressee or intended recipient or a member of the intended audience of

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

4 (10) “Subscriber information” means the name, names of additional
5 account users, account number, billing address, physical address, e-mail
6 address, telephone number, payment method, record of services used, and
7 record of duration of service provided or kept by a service provider regarding a
8 user or account.

9 § 8102. LIMITATIONS ON COMPELLED PRODUCTION OF

10 ELECTRONIC INFORMATION

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

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

16 (1) pursuant to a warrant;

17 (2) pursuant to a judicially recognized exception to the warrant
18 requirement;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18 (e) A warrant or subpoena directed to a service provider shall be
19 accompanied by an order requiring the service provider to verify the
20 authenticity of electronic information that it produces by providing an affidavit

1 that complies with the requirements of Rule 902(11) or 902(12) of the
2 Vermont Rules of Evidence.

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

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

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

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

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

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

20 (3) A law enforcement officer reasonably believes that the information
21 relates to an investigation into child exploitation and the information is

1 retained as part of a multiagency database used in the investigation of similar
2 offenses and related crimes.

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

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

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

4 (2) require an entity that provides electronic communications services to
5 its officers, directors, employees, or agents for the purpose of carrying out their
6 duties to disclose protected user information associated with an electronic
7 communication to or from an officer, director, employee, or agent of the
8 entity; or

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

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

14 § 8103. RETURNS AND SERVICE

15 (a) Returns.

16 (1) If a warrant issued pursuant to section 8102 of this title is executed or
17 electronic information is obtained in an emergency under subdivision
18 8102(b)(4) of this title, a return shall be made within 90 days. Upon
19 certification by a law enforcement officer, an attorney for the State, or any
20 other person authorized by law that an investigation related to the warrant or
21 the emergency is ongoing, a judicial officer may extend the 90-day period for

1 making the return for an additional period that the judicial officer deems
2 reasonable.

3 (2) A return made pursuant to this subsection shall identify:

4 (A) the date the response was received from the service provider;

5 (B) the quantity of information or data provided; and

6 (C) the type of information or data provided.

7 (b) Service.

8 (1) At the time the return is made, the law enforcement officer who
9 executed the warrant under section 8102 of this section or obtained electronic
10 information under subdivision 8102(b)(4) of this section shall serve a copy of
11 the warrant on the subscriber to the service provider, if known. Service need
12 not be made upon any person against whom criminal charges have been filed
13 related to the execution of the warrant or to the obtaining of electronic
14 information under subdivision 8102(b)(4) of this section.

15 (2) Upon certification by a law enforcement officer, an attorney for the
16 State, or any other person authorized by law that an investigation related to the
17 warrant is ongoing, a judicial officer may extend the time for serving the return
18 for an additional period that the judicial officer deems reasonable.

19 (3) Service pursuant to this subsection may be accomplished by:

20 (A) delivering a copy to the known person;

1 (B) leaving a copy at the person’s residence or usual place of abode
2 with an individual of suitable age and discretion who resides at that location;

3 (C) delivering a copy by reliable electronic means; or

4 (D) mailing a copy to the person’s last known address.

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

8 § 8104. EXCLUSIVE REMEDIES FOR A VIOLATION OF THIS
9 CHAPTER

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

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

17 (c) A service provider who receives a subpoena issued pursuant to this
18 chapter may file a motion to quash the subpoena. The motion shall be filed in
19 the court that issued the subpoena before the expiration of the time period for
20 production of the information. The court shall hear and decide the motion as
21 soon as practicable. Consent to additional time to comply with process under

1 section 806 of this title does not extend the date by which a service provider
2 shall seek relief under this subsection.

3 § 8105. EXECUTION OF WARRANT FOR INFORMATION KEPT BY
4 SERVICE PROVIDER

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

15 § 8106. SERVICE PROVIDER’S RESPONSE TO WARRANT

16 (a) The service provider shall produce the items listed in the warrant within
17 30 days unless the court orders a shorter period for good cause shown, in
18 which case the court may order the service provider to produce the items listed
19 in the warrant within 72 hours. The items shall be produced in a manner and
20 format that permits them to be searched by the law enforcement officer.

1 (b) This section shall not be construed to limit the authority of a law
2 enforcement officer under existing law to search personally for and locate
3 items or data on the premises of a Vermont service provider.

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

7 § 8107. CRIMINAL PROCESS ISSUED BY VERMONT COURT;

8 RECIPROCITY

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

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

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

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

3 § 8108. REAL TIME INTERCEPTION OF INFORMATION PROHIBITED

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

12 * * * Automated License Plate Recognition Systems * * *

13 Sec. 6. EXTENSION OF SUNSET

14 2013 Acts and Resolves No. 69, Sec. 3, as amended by 2015 Acts and
15 Resolves No. 32, Sec. 1, is further amended to read:

16 Sec. 3. EFFECTIVE DATE AND SUNSET

17 * * *

18 (b) Secs. 1–2 of this act, 23 V.S.A. §§ 1607 and 1608, shall be repealed
19 on July 1, ~~2016~~ 2019.

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

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

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

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

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

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

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

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

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

9 § 1607. AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS

10 (a) Definitions. As used in this section:

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

17 (2) “Automated license plate recognition system” or “ALPR system”
18 means a system of one or more mobile or fixed high-speed cameras combined
19 with computer algorithms to convert images of registration plates into
20 computer-readable data.

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

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

12 (5) “Legitimate law enforcement purpose” applies to access to active or
13 historical data and means investigation, detection, analysis, or enforcement of a
14 ~~crime, traffic violation, or parking violation~~ or of a commercial motor vehicle
15 violation or defense against the same, or operation of AMBER alerts or
16 missing or endangered person searches.

17 (6) “Vermont ~~Information and Analysis~~ Technology Center Analyst”
18 means any sworn or civilian employee who through his or her employment
19 with the Vermont ~~Information and Analysis~~ Technology Center (~~VTIAC~~)
20 (VTC) has access to secure databases that support law enforcement
21 investigations.

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

4 (c) ALPR use and data access; confidentiality.

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

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

15 (C)(i) Requests to ~~review~~ access active data shall be in writing and
16 include the name of the requester, the law enforcement agency the requester is
17 employed by, if any, and the law enforcement agency's Originating Agency
18 Identifier (ORI) number. ~~The~~ To be approved, the request shall describe the
19 legitimate law enforcement purpose must provide specific and articulable facts
20 showing that there are reasonable grounds to believe that the data are relevant
21 and material to an ongoing criminal, missing person, or commercial motor

1 vehicle investigation or enforcement action. The written request and the
2 outcome of the request shall be transmitted to ~~VTIAC~~ VTC and retained by
3 ~~VTIAC~~ VTC for not less than three years.

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

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

16 (B) Requests for historical data, whether from Vermont or out-of-
17 state law enforcement officers or other persons, shall be made in writing to ~~an~~
18 ~~analyst at VTIAC~~ a VTC analyst. The request shall include the name of the
19 requester, the law enforcement agency the requester is employed by, if any,
20 and the law enforcement agency's ORI number. ~~The~~ To be approved, the
21 request ~~shall describe the legitimate law enforcement purpose~~ must provide

1 specific and articulable facts showing that there are reasonable grounds to
2 believe that the data are relevant and material to an ongoing criminal, missing
3 person, or commercial motor vehicle investigation or enforcement action.

4 ~~VTIAC~~ VTC shall retain all requests and shall record in writing the outcome of
5 the request and any information that was provided to the requester or, if
6 applicable, why a request was denied or not fulfilled. ~~VTIAC~~ VTC shall retain
7 the information described in this subdivision (c)(2)(B) for no fewer than three
8 years.

9 (d) Retention.

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

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

1 retained beyond the 18-month period pursuant to a preservation request made
2 or disclosure order issued under Section 1608 of this title or pursuant to a
3 warrant issued under Rule 41 of the Vermont or Federal Rules of Criminal
4 Procedure.

5 (e) Oversight; rulemaking.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 § 1608. PRESERVATION OF DATA

8 (a) Preservation request.

9 (1) A law enforcement agency or the Department of Motor Vehicles or
10 other person with a legitimate law enforcement purpose may apply to the
11 Criminal Division of the Superior Court for an extension of up to 90 days of
12 the 18-month retention period established under subdivision 1607(d)(2) of this
13 title if the agency or Department offers specific and articulable facts showing
14 that there are reasonable grounds to believe that the captured plate data are
15 relevant and material to an ongoing criminal or missing persons investigation
16 or to a pending court or Judicial Bureau proceeding involving enforcement of a
17 crime or of a commercial motor vehicle violation. Requests for additional 90-
18 day extensions or for longer periods may be made to the Superior Court subject
19 to the same standards applicable to an initial extension request under this
20 subdivision.

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

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

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

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

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

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

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

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

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

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

4 (2) all three of the following apply:

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

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

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

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

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

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

19 § 848. RULES REPEAL; OPERATION OF LAW

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

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

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

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

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

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

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

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

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

