Senate Calendar

TUESDAY, JANUARY 12, 2016

SENATE CONVENES AT: 9:30 A.M.

TABLE OF CONTENTS

Page No.

NOTICE CALENDAR

Second Reading

Favorable with Recommendation of Amendment

ORDERS OF THE DAY

NOTICE CALENDAR

Second Reading

Favorable with Recommendation of Amendment

S. 155.

An act relating to privacy protection.

Reported favorably with recommendation of amendment by Senator Ashe for the Committee on Judiciary.

The Committee recommends that the bill be amended as follows:

First: By striking out Sec. 1 in its entirety and inserting in lieu thereof a new Sec. 1 to read as follows:

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).

Second: In Sec. 2, in 20 V.S.A. § 4622, by striking out subsection (a) in its entirety and inserting in lieu thereof a new subsection (a) to read as follows:

(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.

Third: In Sec. 2, in 20 V.S.A. § 4624, by striking out § 4624 in its entirety and inserting in lieu thereof a new § 4624 to read as follows:

§ 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.

Fourth: By inserting a new Sec. 4 to read as follows:

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.

Fifth: By inserting a new Sec. 5 to read as follows:

* * * 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.

Sixth: By striking out Sec. 6 in its entirety and inserting in lieu thereof the following:

Sec. 8. EFFECTIVE DATE

This act shall take effect on October 1, 2016.

And by renumbering the remaining sections to be numerically correct.

(Committee vote: 5-0-0)

NOTICE OF JOINT ASSEMBLY

January 21, 2016 - 2:00 p.m. – House Chamber – Budget Address by the Honorable Peter E. Shumlin, Governor of the State of Vermont.