TO THE HOUSE OF REPRESENTATIVES:

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

* * * 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.~~

(1) "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.

(2) "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.

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

(4) "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.

(5) "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

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

(7) "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.

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

(9) "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.

(10) "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 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. RETURNS AND SERVICE

(a) Returns.

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

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

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

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

(C) the type of information or data provided.

(b) Service.

(1) At the time the return is made, the law enforcement officer who executed the warrant under section 8102 of this section or obtained electronic

information under subdivision 8102(b)(4) of this section shall serve a copy of the warrant on the subscriber to the service provider, if known. Service need not be made upon any person against whom criminal charges have been filed related to the execution of the warrant or to the obtaining of electronic information under subdivision 8102(b)(4) of this section.

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

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

(A) delivering a copy to the known person;

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

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

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

(c) 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.

§ 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

(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.

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE