TO: **Members of the House Judiciary Committee**
FROM: **Allen Gilbert, executive director, ACLU-VT**
DATE: **April 14, 2016**
SUBJECT: **S. 155, privacy bill**

The right to be free from unreasonable search and seizure is a fundamental right established in the Fourth Amendment to the U.S. Constitution and in Article XI of the Vermont Constitution. That right – born and developed in New England – has served Vermont well for more than 200 years.

Today, however, the right to be free from unreasonable search and seizure is at a crossroads. Our privacy laws no longer fit the way we live in the 21st century, when our "papers and effects" that the founders and Constitution writers were determined to protect are now largely in digital form. Some of our most private and important personal information is no longer physical property kept in our homes, but rather a combination of deliberately and automatically generated electronic information held by service providers.

Additionally, new high-tech tools such as drones and automated license plate recognition systems offer surveillance opportunities that could never have been imagined 200 years ago. Our whereabouts can now be easily tracked by these devices as well as by devices such as cell phones that we carry with us. We have become subjects of observation in this century, and our privacy rights have not caught up with this reality.

The ACLU-VT strongly supports S. 155, but we have some concerns about specific pieces. We provide our comments grouped around the four main topics of the bill – health care records, drones, electronic communications, and automated license plate recognition systems. Underlined text within the statutory language is our additions, and strike-throughs our deletions, to the existing language of the bill as it passed the Senate.

ACLU-VT Testimony on S. 155, April 14, 2016, House Judiciary Committee

Topic 1 – Health Care Records, page 1 of the bill

The Senate Judiciary Committee rejected creation of a private right of action for patients whose medical records are disclosed by a "covered entity" (HIPAA's term for health care facilities). Common throughout many statutes, a private right of action creates a specific mechanism for enforcing a law through court action that a private citizen can take. Such a provision was in the original Senate bill but was eliminated on the last day of the committee's consideration of the bill following testimony from health care industry representatives.

- We believe a private right of action should be added back to the bill, with modification. The reason is this: Vermont's health information exchange has weak front-end protections against unauthorized access to personal medical records. The watchdog agency to which patients can complain about unauthorized access (the federal Office for Civil Rights, or "OCR") focuses its enforcement activity on large breaches. An investigation by National Public Radio and the investigative journalism site ProPublica in 2015 "detailed how the Office for Civil Rights (OCR) only rarely imposed sanctions for small-scale privacy breaches that caused lasting harm." What we want to get at are these small-scale breaches that escape OCR's attention — where a person who, by virtue of his or her position, gains access to the records of one or more other persons, often for personal reasons and often for harmful purposes. We have narrowed the original bill language by targeting the breachers themselves and not the entities they work for, and by prohibiting class action lawsuits and requiring that the violation be intentional or negligent. We believe this narrowing addresses the concerns previously raised by the health care industry representatives while allowing some measure of recovery for breaches that largely go unremedied today. This is done in a new § 1882 in Sec. 1. It is noted below. Other changes are also needed in § 1881 to subsections (a) and (b) for this addition. That language also appears below.

- Also, we suggest creation of a reporting requirement for medical records privacy complaints and breaches by adding two new subsections to § 1881. Covered entities would be required to annually report the number of breaches they experienced. The state Attorney General's Office – which can now also receive complaints – would similarly report annually on breach complaints it receives.

We believe Vermonters deserve these tools so the privacy of medical records is better protected. Underlined text within the statutory language is our additions, and strike-throughs our deletions, to the existing language of the bill as it passed the Senate.

§ 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.

(3) "Use" shall have the same meaning as in 45 C.F.R. § 160.103.

(4) "Disclosure" shall have the same meaning as in 45 C.F.R. § 160.103.

(5) "Business associate" shall have the same meaning as in 45 C.F.R. § 160.103.

(b) ~~A covered entity~~An employee of a covered entity or its business associates shall not use or disclose protected health information unless the use or disclosure is permitted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

(c) A covered entity and its business associates shall report annually on their public websites the number of breaches, if any, that have occurred at the entity or associates within the last 12 months.

(d) The state Attorney General's Office shall report annually on its public website the number of medical records breach complaints it has received within the last 12 months, the number of complaints that resulted in investigations, the results of the investigations that were done, and the sanctions (if any) imposed in each case that was investigated.

§ 1882. PRIVATE CAUSE OF ACTION

(a) A person may bring an action in the Civil Division of the Superior Court for damages, injunctive relief, punitive damages, and reasonable costs and attorney's fees against an employee of a covered entity or its business associates who has intentionally or negligently used or disclosed protected health information in violation of subsection 1881(b) of this title. The court may issue an award for the greater of the person's actual damages or $500.00 for a first violation or $1000.00 for each subsequent violation.

(b) Except as provided in subsection (c) of this section, this section shall not limit any other claims a person may have under applicable law.

(c) A person bringing an action pursuant to subsection (a) shall bring the action in an individual capacity only and shall not bring an action on behalf of a class or in a representative capacity.

ACLU-VT Testimony on S. 155, April 14, 2016, House Judiciary Committee

Topic 2 – Drones, page 1 of the bill

- The ACLU believes this section of S. 155 allows for the responsible use of drones by police, in both regular police work as well as emergency situations. We feel, however, that a specific prohibition against surveillance of First Amendment activities should be added. We suggest subsection (a) under § 4622 on page 2 of the bill be modified:

  > (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. Under no circumstances shall a drone be used to track, collect, or maintain information about the political, religious, or social views, associations, or activities of any individual, group, association, organization, corporation, business or partnership, or other entity unless such information relates directly to investigation of criminal activity and there are reasonable grounds to suspect the subject of the information is involved in criminal conduct.

- We also believe the bill correctly leaves to the Federal Aviation Administration (FAA) the regulation of the use of drones by private operators, with reference to the Academy of Model Aeronautics National Model Aircraft Safety Code.

ACLU-VT Testimony on S. 155, April 14, 2016, House Judiciary Committee

Topic 3 -- Electronic Communications, page 7 of the bill

The Senate Judiciary Committee originally planned for this portion of the bill to be based on the California Electronic Communications Privacy Act, which was passed in the fall of 2015. The California law was developed with broad participation from tech firms, privacy advocates, police, and prosecutors. It has emerged as a national model. Vermont prosecutors felt, however, significant changes were needed to accommodate existing Vermont practices and statutes and allow for greater law enforcement access to electronic communication information. The ACLU, which supported the California model, and representatives from the state's attorneys and attorney general's office were tasked with finding language acceptable to both. Great progress was made, but a few points of contention remained. We continue to feel the following changes should be made:

- The ACLU urges that Vermont follow the California law in requiring a warrant before police may obtain a user's IP (internet protocol) address. We suggest § 8101 on pages 8-9 be modified to read:

> (9) "Protected user information" means I.P. addresses and 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.
>
> (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, and record of duration of service provided~~, and I.P. address~~ kept by a service provider regarding a user or account.

- The ACLU wanted law enforcement to annually report details of their access to electronic information under this chapter. The state's attorneys did not. We believe it's important that people know how frequently law enforcement is getting electronic information under the various provisions of this bill so we can determine whether additional restrictions may, in the future, be appropriate. Because law enforcement is already required to annually report warrants sought and obtained, it should not be too difficult for them to report this subset of warrants. In addition, because, in the Senate version of the bill, police can get so much sensitive information with just a subpoena, we believe use of subpoenas under this chapter should also be reported. This can be accomplished with the addition of this section:

§ 8109. ANNUAL REPORTING REQUIREMENT

(a) A law enforcement agency that obtains electronic information pursuant to this chapter shall make an annual report to the Attorney General. The report shall be made on or before February 1, 2018, and each February 1 thereafter. To the extent it can be reasonably determined, the report shall include all of the following:

(1) The total number of times electronic information was sought or obtained pursuant to this chapter.

(2) For each of the following types of information, the number of times such information was sought or obtained, and the number of records obtained:

(A) Protected user information.

(B) Subscriber information.

(C) Other information kept by a service provider.

(3) For each of the types of information listed in paragraph (2), all of the following:

(A) The number of times that type of information was sought or obtained pursuant to:

(i) Search warrants obtained pursuant to this chapter.

(ii) Emergency requests subject to subsection (h) of section 8102 of this chapter.

(iii) Subpoenas or court orders.

(iv) Judicially recognized exceptions to the warrant requirement.

(v) The lawful user's specific consent.

(B) The total number of individuals whose information was sought or obtained.

(C) For demands or requests issued upon a service provider, the number of such demands or requests complied with in full, partially complied with, and refused.

(D) The number of times notice to targeted individuals was delayed and the average length of the delay.

(E) The number of times electronic information obtained pursuant to this chapter led to a conviction, and the number of instances where electronic information was sought or obtained that was relevant to the criminal proceedings leading to those convictions.

(b) On or before April 1, 2018, and each April 1 thereafter, the Attorney General's office shall publish on its Internet Web site both of the following:

(1) The individual reports from each government entity that requests or compels the production of contents or records pertaining to an electronic communication or location information.

(2) A summary aggregating each of the items in paragraphs (1)-(3) of subsection (a).

(c) Nothing in this chapter shall prohibit or restrict a service provider from producing an annual report summarizing the demands or requests it receives under this chapter.

ACLU-VT Testimony on S. 155, April 14, 2016, House Judiciary Committee

Topic 4 -- Automated License Plate Recognition systems (ALPRs), page 20 of the bill

As was the case two years ago when the first ALPR bill was passed, the retention period of data collected by the systems became the sticking point in consideration of this section of S. 155.

- The ACLU continues to believe that ALPRs should be used only as originally intended – to catch drivers with outstanding warrants, suspended licenses, or unpaid traffic tickets who are on digital "hot lists" distributed regularly by government agencies. ALPRs should not be used as a statewide surveillance system. Data should be deleted after 24 hours. Police can request preservation orders to retain data for longer periods. The only change needed to shorten the retention period is in subsection (d)(1) on page 24 of the bill:

  > (1) A person shall not retain captured plate data for more than ~~18 months~~ 24 hours after the date of its creation unless….

- Retention up to the current 18 months or even longer has been advocated as an exculpatory tool – a tool for innocent people to prove their innocence. This creates what some term a "rainy day" data pool that's there "just in case." This is offensive on two levels: government is not supposed to be collecting and retaining information on people not suspected of criminal activity, and it is a basic right in our criminal justice system to be presumed innocent. Government has the burden to prove someone's guilt; an individual does not have the burden to prove his or her innocence. Once government premises the collection and retention of information about people on the slim chance that it could possibly be exculpatory in some future prosecution, there is no end to what information government might collect about us "just in case." It is a rationale for broad, comprehensive video surveillance, drone surveillance, internet surveillance, or any other dragnet approach to recording citizens' actions. The ACLU believes such a rationale is the antithesis of protecting individuals' privacy.

If you reject a 24-hour retention period in favor of the 18-month period in the Senate bill, we would ask that a warrant or subpoena be required before access to the retained data is allowed. This can be accomplished by modifying subsection (c)(2) on page 23 of the bill as follows:

> (A) Upon ~~request~~receipt of a warrant or a subpoena issued by a judicial officer, who shall issue the subpoena if the requester offers specific and articulable facts showing that the data are sought for a legitimate law enforcement purpose, the Department may disclose captured plate data lawfully retained under this section ~~for a legitimate law enforcement purpose~~. A receiving

person may use the data or further disclose it, but only for a legitimate law enforcement purpose.

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

Private data companies are amassing huge databases of ALPR data. The largest commercial system, according to the *Washington Post*, is Vigilant Solutions. It holds more than 2.5 billion records, and its database adds 2.7 million records a day. The bill prohibits private use of ALPR systems, but some Committee members have raised concerns about the constitutionality of this prohibition. We suggest, if the Committee wishes to avert a possible constitutional challenge, the following changes to subsection (b)(1) on page 22 of the bill be made:

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

Although we might not be able to prohibit private entities from using ALPR systems in Vermont, we can prohibit law enforcement from using the data that private entities collect. This can be accomplished by modifying subsection (e) (on page 24 of the bill) and adding a new section:

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

(f) Data received from a private person. A law enforcement officer may not obtain, receive, review, or use captured plate data from a private person.

(Successive sub-sections must be re-numbered, starting with the old "f".)

We also believe it's important to add language that prohibits law enforcement from using ALPR systems that capture images of the driver and others in the car. Some new systems are capable of doing this, according to the *Washington Post*. This can be accomplished by making these changes to subsection (b)(1) (page 22 of the bill):

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

(A) the officer is certified in ALPR operation by the Vermont Criminal Justice Training Council; ~~and~~
(B) the system automatically transfers captured plate data to the statewide ALPR server maintained by the Department and captured plate data are automatically deleted from the system after the data's transfer to the Department~~.~~; and
(C) the system is not capable of capturing, or is operated in such a way as to prevent capturing, images of occupants of any vehicle.

Finally, we believe that ALPR data obtained or retained in violation of this section must not be used against a criminal defendant. We suggest adding the following two provisions to subsection (g) (page 25 of the bill), which can be renamed "Penalties and remedies":

(3) A defendant in a trial, hearing, or proceeding may move to suppress captured plate data obtained or retained in violation of the U.S. Constitution, the Vermont Constitution, or this chapter.
(4) A defendant in a trial, hearing, or proceeding shall not move to suppress captured plate data on the ground that the constitutional or statutory privacy rights of an individual other than the defendant were violated.