Act No. 169 (S.155). Judiciary; public records; executive branch

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

This act:

- Health Care Privacy. Tracks existing privacy protections contained in the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) by prohibiting, as a matter of State law, health care providers, insurers, and others (defined as "covered entities") from disclosing information about a person's health condition and treatment (defined as "protected health information").

- Drones. Prohibits law enforcement agencies from using drones or information acquired through the use of a drone for the purpose of investigating, detecting, or prosecuting crime unless the agency has obtained a warrant or unless one of the court-recognized exceptions to the warrant requirement applies. Prohibits law enforcement agencies from using drones to gather or retain data on private citizens peacefully exercising their constitutional rights of free speech and assembly, unless the drone is being used either: (1) for observational, public safety purposes that do not involve gathering or retaining data; or (2) pursuant to a warrant. Law enforcement agencies are permitted to use drones operated for purposes other than the investigation, detection, or prosecution of crime, including search and rescue operations and aerial photography for the assessment of accidents, forest fires and other fire scenes, flood stages, and storm damage. Prohibits any person from equipping a drone with a dangerous or deadly weapon or from firing a projectile from a drone.

- Electronic Communications. Establishes the Vermont Electronic Communications Privacy Act (VECPA), which addresses law enforcement access to e-mails, communications data, and other records held by electronic communications companies. Requires law enforcement to obtain a warrant before accessing "protected user information" (content, location data, and the subject line of e-mails), and permits law enforcement to use a standard subpoena to obtain "subscriber information" (data about the communication, such as names and e-mail addresses of senders and recipients, account numbers, payment information, etc.). Information that does not fall into either category of protected user information or subscriber information, such as IP addresses, is subject to a heightened subpoena standard and may only be obtained if the information is relevant to an offense or reasonably calculated to lead to the discovery of evidence of the offense. Disclosure of protected information without a warrant is permitted under four circumstances: (1) pursuant to an existing, judicially recognized exception to the warrant requirement; (2) if the user consents; (3) in an emergency involving danger of death or serious bodily injury to

any person; or (4) if the device is seized from an inmate's possession or found in a correctional facility or court to which inmates have access, and the device is not in the possession of an individual or an authorized visitor to the facility. When the service provider turns the information over to the law enforcement officer, the officer must contemporaneously notify the person who is the target of the warrant. The officer may motion the court to delay this notice requirement for 90 days (and for additional 90-day periods by filing subsequent motions) if the court finds that notification would jeopardize an investigation, endanger a person's life or physical safety, or cause some other adverse result.

- Sunset of Laws Governing Use of Automated License Plate Recognition (ALPR) Systems and Data. Extends by two years, from July 1, 2016 to July 1, 2018, the repeal of 23 V.S.A. §§ 1607 and 1608, which regulate the use of ALPR systems and the use and retention of ALPR data.
- Analysis of ALPR System-Related Costs and Benefits. Directs the Department of Public Safety, in consultation with the Joint Fiscal Office, to analyze all present and projected costs associated with ALPR systems used by law enforcement in Vermont and conduct a cost-benefit analysis of the use of the systems, and to report its findings to the House and Senate Committees on Judiciary and on Transportation on or before January 15, 2017.
- Amendments to Laws Governing Law Enforcement Use of ALPR Systems and Data. Amends the existing law governing the use of ALPR systems and the use and retention of ALPR data to provide that: a "legitimate law enforcement purpose" for the use of ALPR systems and data includes a person's defense against certain charges and does not include enforcement of parking or traffic violations other than commercial motor vehicle violations; access to active ALPR data stored on individual ALPR units and to historical data stored on the statewide database maintained by the Department of Public Safety will require a person to cite "specific and articulable facts showing that there are reasonable grounds to believe that the data are relevant and material to an ongoing criminal, missing person, or commercial motor vehicle investigation or enforcement action"; access to historical ALPR data will be governed by this standard for the first six months after the data's creation and that after six months, the data will only be accessible pursuant to a warrant if not requested in connection with a pending criminal charge or pursuant to a court order by the prosecution or the defense in connection with a pending criminal charge; and the Department of Motor Vehicles, in connection with commercial motor vehicle enforcement activities, may manage a separate database of ALPR data. In addition, the act also amends the existing law to expand the annual reporting requirements of the Department of Public Safety and to require

the Department to adopt rules on or before January 1, 2018 to implement the law.

- Information Related to Use of Ignition Interlock Devices. Provides that data in the custody of a public agency related to the use of an ignition interlock device shall not be disclosed except pursuant to a warrant, in the case of an emergency, or in connection with an enforcement proceeding for violating the law regulating persons who operate under an ignition interlock restricted driver's license.
- Administrative Procedure Act; Code of Administrative Rules. Requires the Secretary of State to publish a code of administrative rules that contains all administrative rules adopted under the Administrative Procedure Act, and provides that an administrative rule in effect on or before July 1, 2016 shall be repealed on July 1, 2018 if it is not published in the code of administrative rules before July 1, 2018.

Effective Date: Multiple effective dates, beginning on June 6, 2016