S.150

Introduced by Senator Vyhovsky

Referred to Committee on

Date:

Subject: Motor vehicles; Department of Motor Vehicles; operator's licenses; mobile identification; privacy

Statement of purpose of bill as introduced: This bill proposes to establish specific requirements to protect the privacy of individuals who use mobile identification and to limit access to images recorded by automated traffic law enforcement systems.

An act relating to privacy protections for mobile identification and images recorded by automated traffic law enforcement systems

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 23 V.S.A § 116 is amended to read:

§ 116. ISSUANCE OF MOBILE IDENTIFICATION

(a) Definitions. As used in this section:

(1) "Attribute authentication" means the verification of a specific quality of a data field on a mobile identification without revealing the underlying data in that field. Attribute authentication includes verifying that a mobile

identification holder is legally permitted to purchase an age-restricted item without revealing the holder's date of birth or actual age.

(2) "Data field" means a discrete piece of information that appears on a mobile identification.

~~(2)~~(3) "Full profile" means all the information provided on a mobile identification.

~~(3)~~(4) "Limited profile" means a portion of the information provided on a mobile identification.

~~(4)~~(5) "Mobile identification" means an electronic representation of the information contained on a nonmobile credential.

~~(5)~~(6) "Mobile identification holder" means an individual to whom a mobile identification has been issued.

~~(6)~~(7) "Nonmobile credential" means a nondriver identification card issued under section 115 of this title, a driver's license issued under section 603 of this title, a junior operator's license issued under section 602 of this title, a learner's permit issued under section 617 of this title, a commercial driver's license issued under section 4111 of this title, or a commercial learner's permit issued under section 4112 of this title.

(8) "Selective disclosure" means the disclosure through a verification system of only certain data fields from a mobile identification that are

reasonably necessary for the purposes of the verification and the ability of the mobile identification holder to determine which data fields are disclosed.

(b) Issuance. The Commissioner of Motor Vehicles may issue a mobile identification to an individual in addition to, and not instead of, a nonmobile credential. If issued, the mobile identification shall:

(1) be capable of producing both a full profile and a limited profile;

(2) satisfy the purpose for which the profile is presented;

(3) allow the mobile identification holder to maintain physical possession of the device on which the mobile identification is accessed during verification; and

(4) not be a substitute for an individual producing a nonmobile credential upon request.

* * *

(d) Administration.

(1) The Commissioner may operate, or may operate through a third-party administrator, a verification system for mobile identifications.

(2) Access to the verification system and any data field by a person presented with a mobile identification requires the ~~credential~~ mobile identification holder's consent, and, if consent is granted, the Commissioner may release the following through the verification system:

(A) for a full profile, all data fields that appear on the mobile identification; and

(B) for a limited profile, only the data fields ~~represented in the limited profile for~~ appearing on the mobile identification that the mobile identification holder has consented to have released.

(3) The Commissioner shall ensure that any verification system for mobile identifications meets the following requirements:

(A) The verification system does not incentivize or require a person using the verification system to take possession of a mobile identification holder's device while accessing data from the mobile identification.

(B) The verification system does not share or retain any information regarding the persons that have accessed data from a particular mobile identification or the locations at which data from a particular mobile identification has been accessed.

(C) The verification system requires attribute authentication or selective disclosure in all instances when access to a full profile is not reasonably necessary. The verification system shall ensure that the data fields being requested are first disclosed to the mobile identification holder and that the mobile identification holder may determine which data fields are released to the person requesting the data.

(D) The verification system utilizes techniques, methodologies, or processes that ensure that data obtained from a mobile identification, including the fact that the verification system was accessed in relation to a specific mobile identification, cannot be linked together by one or more persons who access the verification system.

(4)(A) The Commissioner shall adopt standards relating to:

(i) security and communications requirements for devices on which mobile identifications are stored;

(ii) procedures for requesting and accessing data from mobile identifications through the verification system;

(iii) minimum requirements for the identification and authentication of the mobile identification holder prior to obtaining the identification holder's consent to the disclosure of data fields on the mobile identification; and

(iv) requirements providing for the storage of information regarding what data was requested and accessed from a mobile identification, which shall only be available to the mobile identification holder and may be retained or destroyed at the mobile identification holder's discretion.

(B) The standards, to the extent practicable, shall be based on widely accepted and publicly available national or international standards.

(e) Privacy protections.

(1) The verification system and mobile identifications shall not permit the Department or any State entity to obtain control over the device on which a mobile identification is stored or to deactivate a mobile identification stored on a mobile identification holder's device.

(2) A law enforcement officer shall not take physical possession of the device on which a mobile identification holder's mobile identification is accessed for the purpose of accessing the mobile identification or verifying the mobile identification holder's identity.

(3) No person shall request more data from a mobile identification than is reasonably necessary to determine that the mobile identification holder meets the legal requirements to enter into the transaction with the person requesting the data.

(4) No digital services provider, application developer, or administrator or operator of the verification system shall access, collect, retain, share, or use data from a mobile identification or data about the use of a mobile identification, except as necessary to comply with applicable State and federal law.

(f) Right to choose whether to use mobile identification.

(1) No person shall condition the offer or use of a good or service on access to an individual's mobile identification or nonmobile credential except if:

(A) the transaction requires proof of age, identity, residency, or another characteristic pursuant to State or federal law;

(B) the identification or credential is requested in relation to financial or banking services to ensure that accounts, funds, financial instruments, or personally identifiable information or financial data is not accessed by an unauthorized person; or

(C) the identification or credential is requested in relation to medical services to ensure that goods, services, or private medical information are not provided to an unauthorized person.

(2) No person shall charge different prices or rates for goods or services, provide different treatment or quality of goods or services, or condition access or entry to a location based on whether an individual presents mobile identification or an appropriate nonmobile credential, unless the use of mobile identification or an appropriate nonmobile credential is necessary for conducting a remote transaction or due to circumstances beyond the person's control that prevent the person from accessing the verification system.

(g) Enforcement.

(1) The Attorney General or a State's Attorney may bring an action against a private entity to enforce the provisions of this section by restraining prohibited acts, seeking civil penalties, obtaining assurances of discontinuance, and conducting civil investigations in accordance with the procedures

established in 9 V.S.A. §§ 2458–2461 as though a violation of the provisions of this section is an unfair act in commerce. Any person complained against shall have the same rights and remedies as specified in 9 V.S.A. §§ 2458–2461. The Superior Courts are authorized to impose the same civil penalties and investigation costs and to order other relief to the State of Vermont or an aggrieved individual for violations of this section as they are authorized to impose or order under the provisions of 9 V.S.A. §§ 2458 and 2461 in an unfair act in commerce.

(2) An individual who has been aggrieved by a violation of the provisions of this section may bring a civil action in the Superior Court seeking:

(A) damages equal to:

(i) for a negligent violation of the provisions of this section, $2,500.00 or the amount of actual damages, whichever is greater; and

(ii) for an intentional violation of the provisions of this section, $5,000.00 or the amount of actual damages, whichever is greater;

(B) restraint of prohibited acts;

(C) reasonable attorney's fees and costs; and

(D) other appropriate relief.

(3) For purposes of enforcing the provisions of this section, a repeated violation of the provisions of this section by the same person through identical

use of the same individual's mobile identification prior to enforcement under the provisions of this subsection shall not constitute separate violations of the provisions of this section.

Sec. 2. 23 V.S.A. § 1606 is amended to read:

§ 1606. AUTOMATED TRAFFIC LAW ENFORCEMENT SYSTEMS; SPEEDING

* * *

(b) Vendor.

(1) The Agency of Transportation shall enter into a contract with a third party for the operation and deployment of ATLE systems on behalf of the Agency.

(2) The Agency, in consultation with the Department of Public Safety, may require the vendor to maintain a storage system to store any recorded images or other data collected by the ATLE system. Any storage system shall adhere to the use, retention, and limitation requirements pursuant to this section.

(3) The Agency, in consultation with the Department of Public Safety, shall require the vendor to employ security measures to prevent the disclosure of any recorded images for any reason other than the issuance and adjudication of a civil violation complaint to enforce the provisions of this section and the resolution of any related appeal.

* * *

(l) Limitations.

(1) ATLE systems shall only record violations of this section and shall not be used for any other purpose, including other surveillance purposes.

(2) Recorded images shall only be accessed to determine if a violation of this section was committed in the prior 12 months.

(3) Notwithstanding any applicable law to the contrary, the Agency of Transportation may permit the vendor to coordinate with designated law enforcement agencies to obtain a recorded image from the vendor to determine whether a violation of this section occurred within the prior 12 months.

(4) Recorded images shall not be subject to subpoena or discovery and shall not be admissible in any action except a proceeding to enforce the provisions of this section.

(5) Except as otherwise provided pursuant to the provisions of this section, recorded images shall be kept confidential and are exempt from public inspection and copying under the Public Records Act. Notwithstanding 1 V.S.A. § 317(e), the Public Records Act exemption created pursuant to this subdivision (5) shall continue in effect and shall not be repealed through the operation of 1 V.S.A. § 317(e).

Sec. 3. EFFECTIVE DATE

This act shall take effect on July 1, 2025.