Section by Section Summary

S.110 – An act relating to data privacy and consumer protection

(As passed Senate Economic Development)

Sec. 1 – Privacy Audit

Sec. 1 directs the Chief Data Office (within the Agency of Digital Services) and the Chief Records Officer (within the Secretary of State's office) to deliver a report to committees of jurisdiction on or before January 15, 2020 concerning the collection and management within State government of the personally identifiable information, street addresses, email addresses, telephone numbers, and demographic information of Vermont citizens.

Sec. 2 – Date Breach Notices – Definition of "Personally Identifiable Information"

Vermont's "Security Breach Notice Act" imposes a duty on a data collector to report to the Attorney General and to consumers when a data breach occurs that results in the unauthorized access of "personally identifiable information."

Section 2 amends the statutory definition of "personally identifiable information" to add categories for biometric data, genetic information, health information, login credentials, and passport numbers.

Sec. 3 – Student Online Privacy Protection

In 2014 California adopted SOPIPA – the Student Online Privacy and Information Protection Act, which took effect on January 1, 2016. Since then, over 34 additional states have adopted similar laws.

Sec. 3 adopts a Vermont version of SOPIPA in 9 V.S.A. chapter 62, subchapter 3A. This version is very similar to California's version, with a few updates to clarify definitions for what information is covered and what company practices are subject to the law's application.

The law:

- Applies to "covered information" = information about or generated by a student when using an "operator" educational website, service, or application for "K-12 school purposes." (see § 2443 definitions)

- Subject to certain exceptions (see §§2443c-2443e), prohibits an "operator" from:
    - targeting advertising toward a student through the operator's website, service, or application
    - amassing a profile about the student
    - selling, renting, or bartering a student's information
    - disclosing a student's information
    - see § 2443a

- Requires an operator to:
    - Implement security procedures to protect privacy
    - Delete student's information at a school's request
    - Publicly disclose its information collection and use practices
    - See § 2443b

- Creates a consumer protection violation if an operator fails to follow its requirements (§ 2443f)

Sec. 4 – Date Breach Notices – Substitute Notice

As discussed above in reference to Sec. 2 of this bill, the Security Breach Notice Act requires a data collector to give notice to a consumer if a data breach occurs.

Under current law the data collector must give direct notice by writing, by email, or by telephone (subject to certain conditions), unless the data collector is permitted to use "substitute notice." Substitute notice is currently permitted if:

1. the cost of direct notice exceeds $5,000
2. the class of affected consumers exceeds 5,000; or
3. the data collector does not have sufficient contact information

Section 4 of this bill amends the substitute notice provision:

- to eliminate the exception for consumers classes of over 5,000 people, and
- to permit a data collector to use substitute notice only if:
    1. the data collector demonstrates that the lowest cost of providing notice to affected consumers pursuant to subdivision (6)(A) of this subsection among written, e-mail, or telephonic notice to affected consumers would exceed $10,000.00; or
    2. the data collector doesn't have sufficient contact information