Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology & Economic Development Committee

HB 2200

Brief Description: Protecting the privacy and security of internet users.

Sponsors: Representatives Hansen, Taylor, Smith, Buys, Harmsworth, Graves, Maycumber, J. Walsh, Kraft, Haler, Condotta, Nealey, Bergquist, Steele, Van Werven, Stonier, Macri, Farrell, Cody, Slatter, Tarleton, Senn, Kagi, Pollet, Frame, Chapman, Dye, Hudgins, Stanford, Reeves, Dent, Hayes, Ryu, Peterson, Sells, Kloba, Santos, Johnson, Fitzgibbon, Holy, Ormsby, Caldier, Sawyer, Wylie, Hargrove, Kilduff, Blake, Orcutt, Gregerson, Young, Appleton, Shea, Koster, Morris, Tharinger, Irwin, Muri, Schmick, Volz, Goodman, Clibborn, McCaslin, Pellicciotti, Doglio, Jinkins, Dolan, Kirby, Sullivan, Lytton, Kretz, Riccelli, Rodne, McBride, McCabe and Pettigrew.

Brief Summary of Bill

- Requires broadband Internet providers to provide notice and obtain consent to use, disclose, or permit access to certain customer information.
- Requires broadband Internet providers to provide notice of privacy policies and take reasonable data security measures.
- Requires broadband Internet providers to notify customers following a data breach involving certain customer information.

Hearing Date: 4/12/17

Staff: Lily Smith (786-7175).

Background:

Federal Regulation.
The Federal Communications Commission (FCC) regulates interstate and international communication in promotion of several purposes, including development and provision of services at reasonable rates and promotion of safety of life and property through communications

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

use. The Federal Trade Commission (FTC) is tasked with preventing unfair or deceptive acts or practices in or affecting commerce, except with regard to certain industry sectors.

Prior to 2015, the FCC classified the provision of broadband Internet access services (BIAS) as an information service. The provision of information services is not subject to common carrier regulation by the FCC under the Federal Telecommunications Act. The FTC has authority to enforce privacy and data security for information services through its broad enforcement power over unfair or deceptive acts or practices. The Federal Trade Commission Act restricts the FTC from exercising jurisdiction over common carriers when engaged in business as a common carrier.

In a 2015 order, the FCC reclassified the provision of BIAS as a telecommunications service, subjecting it to common carrier regulation under Title II of the Federal Telecommunications Act. Section 222 of Title II requires telecommunications carriers to protect the confidentiality of customer proprietary information. In the 2015 order, the FCC declined to apply to BIAS providers the majority of the rules previously promulgated under Title II for other telecommunications services providers, including existing rules implementing section 222.

In October 2016, the FCC adopted new rules implementing section 222, and applied them to all telecommunications services, including BIAS. The new harmonized rules used a sensitivity-based framework for customer information, and included requirements regarding:

- notice of privacy policies;
- notice and consent regarding use of, disclosure of, and permitting access to customer information;
- conditioning of service and privacy right waivers; and
- data security and data breach notification.

The 2016 FCC rules did not apply to online services beyond BIAS, such as websites, electronic mail, and music and video streaming services (sometimes referred to as "edge services").

In April 2017, a law enacted through the Congressional Review Act (CRA) repealed the 2016 FCC rules. Issuance of a rule substantially the same as one repealed under the CRA is prohibited unless the rule is specifically authorized by a law enacted after the date of repeal of the original rule.

State Data Breach Law.
Data breach law requires any person or business to notify possibly affected persons when security is breached and personal information is (or is reasonably believed to have been) acquired by an unauthorized person. Disclosure is not required if a breach is not reasonably likely to subject customers to a risk of harm. A consumer injured by a violation of these laws may bring a civil action to recover damages and seek an injunction. The Attorney General may also bring an action for enforcement under the Consumer Protection Act (CPA).

State Consumer Protection Act.
Under the CPA, unfair or deceptive acts or practices in trade or commerce are unlawful. The CPA provides that any person injured in his or her business or property through such practices may bring a civil action to recover actual damages sustained and costs of the suit, including reasonable attorney's fees. Treble damages may also be awarded in the court's discretion,

provided the damage award does not exceed $25,000. The Attorney General may bring an action under the CPA in order to restrain and prevent unfair and deceptive acts and practices.

Summary of Bill:

The notice, consent, security, service, and waiver requirements from the repealed 2016 FCC rules are applied to BIAS providers.

The state data breach notification law is amended to apply to BIAS providers for customer proprietary information ("customer PI") as defined in the repealed FCC rules.

Notice

A BIAS provider must notify customers:

- of privacy policies and any material changes in advance;
- of their right to deny or withdraw access to customer PI at any time;
- of a mechanism for granting, denying, or withdrawing approval;
- that customer decisions regarding customer PI will not affect service; and
- that customer decisions regarding customer PI are valid until affirmatively revoked.

Consent

To use, disclose, or permit access to customer PI, a BIAS provider must obtain:

- customer opt-in approval if the customer PI is sensitive; or
- customer opt-out approval if the customer PI is nonsensitive.

A BIAS provider does not need customer approval to use, disclose, or permit access to customer PI:

- in the provision of or billing for the Internet access service;
- to protect rights or property of the BIAS user, or other users or providers from fraudulent, abusive, or unlawful use of the service;
- to provide marketing and other services in a customer-initiated interaction;
- to provide location or nonsensitive customer PI in specific safety and emergency situations; or
- as otherwise required or authorized by law.

A BIAS provider must obtain opt-in approval to make any material retroactive change that would result in a use, disclosure, or permission of access for which the customer did not previously give approval.

Customer approvals must meet specified notice, timing, form, and content requirements. A BIAS provider must provide customers a mechanism to access the required notices and the mechanism to grant, deny, or withdraw approvals at any time.

Security and Data Breach Notification

A BIAS provider must take reasonable steps to protect customer PI, taking into account the provider's activities and size, sensitivity of the data collected, and technical feasibility.

Existing data breach notification requirements are applied to BIAS providers with regard to customer PI.

Service and Waivers

A BIAS provider may not condition or refuse service as a consequence of a customer's refusal to waive privacy rights. If a BIAS provider offers a financial incentive in exchange for customer approval regarding customer PI, it must obtain opt-in approval and provide additional information regarding the program, other service options, and a mechanism to withdraw approval at any time.

Enforcement

A violation of these requirements is enforceable under the CPA. Receipts from any recoveries by the Attorney General are to be deposited in a new account in the state treasury.

Report

The Office of the Attorney General must submit a report to the Legislature by December 1, 2020, regarding additional opportunities to increase consumer transparency, control, and protection through the regulation of additional industry categories.

Definitions

"Customer proprietary information" means any of the following a carrier acquires in connection with its provision of BIAS:

- individually identifiable customer proprietary network information;
- personally identifiable information; and
- content of communications.

"Sensitive customer proprietary information" includes:

- financial information;
- health information;
- information pertaining to children;
- Social Security numbers;
- precise geolocation information;
- content of communications;
- call detail information; and
- web browsing history, application usage history, and the functional equivalents of either.

Appropriation: None.

Fiscal Note: Requested on April 4, 2017.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.