

HOUSE BILL REPORT

ESHB 2200

As Passed House:
May 25, 2017

Title: An act relating to protecting the privacy and security of internet users.

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

Sponsors: House Committee on Technology & Economic Development (originally sponsored by 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 History:

Committee Activity:

Technology & Economic Development: 4/12/17, 4/14/17 [DPS].

Floor Activity:

Passed House: 4/19/17, 87-10.

First Special Session

Floor Activity:

Passed House: 5/2/17, 79-13.

Second Special Session

Floor Activity:

Passed House: 5/25/17, 72-22.

Brief Summary of Engrossed Substitute Bill

- Requires broadband Internet providers to obtain opt-in consent to sell or transfer certain customer information.
- Requires broadband Internet providers to obtain opt-in consent to send or display an advertisement to a customer based on certain customer information.

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.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 15 members: Representatives Morris, Chair; Kloba, Vice Chair; Tarleton, Vice Chair; Smith, Ranking Minority Member; DeBolt, Assistant Ranking Minority Member; Doglio, Fey, Harmsworth, Hudgins, McDonald, Santos, Slatter, Steele, Wylie and Young.

Minority Report: Without recommendation. Signed by 2 members: Representatives Manweller and Nealey.

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 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 service 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 Consumer Protection Act.

Under the Consumer Protection Act (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 Engrossed Substitute Bill:

A BIAS provider must obtain opt-in consent to sell or transfer customer proprietary information (PI), or to send or display an advertisement to a customer that was selected based on the customer's PI. Approval must be solicited at the time of sale, and new approval must be obtained for changes inconsistent with the terms or conditions at prior approval.

Providers of BIAS must provide a mechanism for a customer to grant, deny, or withdraw approval to: (1) sell or transfer customer PI, or (2) send or display an advertisement to a customer that was selected based on the customer's PI.

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 disclose certain information regarding the use of the information and provide a mechanism to withdraw participation.

A violation of these requirements is enforceable under the CPA.

The Utilities and Transportation Commission (UTC) is authorized to adopt rules further defining the definitions and prescribing appropriate notice to be provided to customers.

The substantive sections of the act expire upon determination by the UTC that the federal government has established BIAS customer protections standards substantially equivalent to the levels of protection provided in the act.

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

- content of communication;
- call detail information;

- financial information;
- health information;
- information pertaining to children;
- Social Security numbers;
- precise geolocation information;
- web browsing history, application usage history, and the functional equivalents of either; and
- other personally identifiable information.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed, except for sections 1 through 7, relating to internet user privacy, which take effect December 31, 2018.

Staff Summary of Public Testimony:

(In support) These requirements would support transparency, privacy, and security. They are necessary until the federal government addresses this issue. There are multiple reasons to treat broadband Internet providers differently from other online companies. Internet providers have taken inconsistent positions on whether the statutory provisions apply to them. The state needs strong technology companies, and those companies rely on informed consumers. Privacy is a fundamental value long recognized by the state. Internet access is a fundamental need and used to conduct a range of daily activities. It is expensive to switch providers, and customers should not need to give up basic privacy to meet basic needs. Internet providers have a lot of power with this information and could use it to discriminate between customers. Nonsensitive information can increasingly reveal significant information about a person, and opt-in consent should apply to all provisions. Allowing Internet providers to give discounts for approvals will disproportionately impact low-income people.

(Opposed) Providers take privacy seriously and have committed to privacy standards that protect information. There has been no loss in privacy protection, and the existing federal framework for the approach to privacy and enforcement makes state legislation unnecessary. This bill would create two different frameworks for content and service providers, and would create confusion for consumers. This is one element of a broader discussion at the federal level, and there is an opportunity at that level to clarify how regulation should proceed. The federal agencies have already committed to continue to protect privacy and take enforcement action. This is a complicated subject, and state legislation is being rushed without engaging stakeholders and understanding the impact. The bill would divert resources and create barriers.

(Other) Privacy is an area where states traditionally regulate, and there is no known preemption issue. The FCC was setting minimum standards in its rule and has been clear that it welcomes state regulation in this area.

Persons Testifying: (In support) Representative Hansen, prime sponsor; Alex Alben, Office of Privacy and Data Protection; Elisabeth Smith, American Civil Liberties Union of Washington; Jared Friend, Hintze Law PLLC; Raven Alder, Electronic Rights Rainier; and Joe Kendo, Washington State Labor Council and American Federation of Labor and Congress of Industrial Organizations.

(Opposed) Tom Gurr, Pacific Technology Alliance; Michael Schutzler, Washington Technology Industry Association; Joanie Deutsch, TechNet; Tom McBride, Computer Technology Industry Association; Kate Lucente, State Privacy and Security Coalition; Ron Main, Broadband Communications Association of Washington; and Robert Battles, Association of Washington Business.

(Other) Alan Copsy, Office of the Attorney General.

Persons Signed In To Testify But Not Testifying: None.