

## HB 2813 A STAFF MEASURE SUMMARY

### House Committee On Rules

---

**Action Date:** 05/16/17

**Action:** Do pass with amendments and be referred to Ways and Means. (Printed A-Eng.)

**Vote:** 6-1-2-0

**Yeas:** 6 - Hack, McLane, Nosse, Rayfield, Smith Warner, Williamson

**Nays:** 1 - Barreto

**Exc:** 2 - Holvey, Kennemer

**Fiscal:** Fiscal impact issued

**Revenue:** No revenue impact

**Prepared By:** Erin Seiler, LPRO Analyst

---

#### WHAT THE MEASURE DOES:

Prohibits broadband Internet access service provider (BIASP) from disclosing, selling or permitting access to customers' personal information unless customer provides express consent. Allows customer to revoke consent at any time. Prohibits BIASP from refusing to provide service, charging higher prices for service or offering discount on service that is contingent on consent. Permits BIASP to disclose personal information for specific reasons including billing and collections, initiating or rendering service, protection of BIASP and customer against fraudulent access to services, complying with court order or for emergency situation when precise location of customer is necessary. Requires BIASP establish administrative, technical and physical safeguards as specified, to protect customers' personal information. Provides private right of action against BIASP if customers' personal information is unlawfully sold, disclosed or made accessible. Creates Task Force on Broadband Security staffed by Legislative Policy and Research Office. Specifies membership, charge and reporting requirements. Declares emergency, effective upon passage.

#### ISSUES DISCUSSED:

- Recent federal action regarding Internet privacy
- Privacy of individual's Internet browsing history and online presence
- Federal Communications Commission (FCC) rulemaking authority
- Ability to access broadband and Internet service in rural community
- Federal regulation versus state-by-state regulation of Internet Service Providers (ISPs)
- Federal Trade Commission (FTC) authority over ISP privacy practices

#### EFFECT OF AMENDMENT:

Replaces measure.

#### BACKGROUND:

Recently, the federal government enacted Senate Joint Resolution 34, invoking the Congressional Review Act (CRA) to repeal Federal Communications Commission (FCC) broadband privacy rules. This repeal eliminated updated privacy rules for broadband providers and established a prohibition that prevents the FCC from reviving identical or "substantially similar" rules in the future. Repealed rules included guidelines for cable and telephone industries to obtain user's consent before selling their personal data such as the websites they visit, the applications they use, and other details that individuals share about themselves when using the Internet. The use of the Congressional Review Act to repeal FCC rules has led to uncertainty about the ability of the FCC to enforce an individual's legal right to communications privacy under Section 222 of the Telecommunications Act of 1996. Federal privacy protection has

## **HB 2813 A STAFF MEASURE SUMMARY**

also been impacted by the Ninth Circuit Court of Appeals' decision in *Federal Trade Commission (FTC) v. AT&T Mobility* (835 F.3d 993 (2016)) where the court found that the FTC is legally prohibited from exerting authority over common carriers due to their exclusion from the FTC Act. In the absence of FCC rules and in light of uncertainties about the FTC's jurisdiction to regulate the exploitation of consumers' personal data by broadband providers, a regulatory void may exist that leaves consumers unprotected.

House Bill 2813-A establishes online privacy protection for customers of broadband Internet access service providers (BIASPs) by prohibiting disclosure, selling or access to customers' personal information without their express consent. Information that may not be disclosed includes a customer's name, address, billing or other financial information and demographic data. In addition, a BIASP cannot disclose information about customers' Internet use, including browsing and application use histories, device identifiers associated with the customer, web addresses to or from which information is sent or received, customers' precise locations and the content of customers' Internet communications, including information pertaining to the customer's finances, health or children.