**Testimony of**
**GERARD KEEGAN**
**CTIA**

**In Opposition to Montana House Bill No. 457**

**Before the Montana House Judiciary Committee**

**March 15, 2019**

Chair Doane and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, I am here in opposition to House Bill No. 457. From the outset, it is important to note that there is no gap in privacy protections that must be filled at the state level. The 2017 Congressional action did not change privacy protections for consumers. The Federal Communications Commission (FCC) rules had not taken effect, so the 2017 Congressional Review Act changed nothing from the privacy framework that previously existed. State-specific ISP privacy legislation, like HB 457, deviates from that framework and imposes unjustified restrictions on ISPs.

Now that the FCC's *Restoring Internet Freedom Order* is in effect, the Federal Trade Commission (FTC) once again has oversight and enforcement authority over ISP consumer privacy practices. For over 20 years, the FTC has developed and enforced an effective privacy framework that applies to all players in the internet ecosystem. Restoring FTC jurisdiction subjects ISPs to the same, effective regulatory framework that applies to the rest of the internet ecosystem.

The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy.[1] Most recently, the FTC, with 32 state attorneys general, brought an action against a large computer manufacturer alleging that it "preinstalled software that interfered with how a user's browser interacted with websites."[2] The Commission also brought charges against a ride sharing company alleging that it failed to "live up to its claims that it closely monitored employee access to consumer and driver data."[3] These are just two examples of more recent FTC privacy enforcement actions. The Montana Attorney General can also bring enforcement actions against ISPs that violate state statutes such as unfair trade practices prohibitions.[4]

HB 457 would create two sets of rules that are different for various entities within the internet ecosystem. This would lead to widespread consumer confusion about which rules apply to their data and work to create an uneven playing field. Internet users overwhelmingly prefer a single national standard. Survey results submitted to the FCC showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules.[5] These findings indicate that state legislation, like HB 457, targeting ISPs would in fact be inconsistent with what consumers actually want.

---

[1] *See* "Privacy & Data Security Update: 2017," *available at*: https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives (Jan. 2018).
[2] *Id.*
[3] *Id.*
[4] E.g., Mont. Code Ann. §§ 30-14-101 through 30-14-142.
[5] https://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf

In addition, ISPs do not have unique access to consumer data. A study by privacy expert Peter Swire found that ISP access to consumer data is not comprehensive, that technological developments place substantial limits on ISP visibility, and ISP access to user data is not unique – other companies have access to more information and a wider range of user information.[6] Consumers no longer use a single stationary device. Today consumers use many connected devices serviced by multiple ISPs.

Research predicts that more than 80 percent of web traffic will be encrypted by the end of the year and that number continues to grow.[7] Google estimates, for example, that 90 percent of traffic over Chrome is encrypted.[8] When a website is encrypted, an ISP does not know what a user views on that site. Additionally, a growing number of consumers use virtual private networks that block ISPs from even seeing the domain name that a user is visiting. There cannot be comprehensive ISP visibility when ISPs are prevented from seeing user activity.

In recognition that the internet is not defined by state lines, the recent FCC order includes preemption language to avoid a patchwork of state laws regulating internet service. The FCC has recognized that "broadband Internet access service should be governed by a uniform set of federal regulations, rather than by a patchwork of

---

[6] *See* "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," *available at:* http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf (Feb. 29, 2016).
[7] *See* Cisco Encrypted Traffic Analytics White Paper, *available at:* https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf (Jan. 2019).
[8] https://transparencyreport.google.com/https/overview?hl=en

separate state and local requirements."[9] Conflicting state rules could hamper the provision of broadband service, lead to increase compliance costs, and inhibit providing new and innovative products and services – all to the detriment of consumers. Finally, despite the introduction of bills similar to HB 457 in over 20 states since 2017, no state has passed an ISP privacy law because states increasingly recognize the unintended consequences and negative repercussions that could result from legislation of this kind.

CTIA strongly supports ongoing efforts within the federal government to develop a uniform national approach to consumer privacy.[10] Several federal agencies, including the Federal Trade Commission (FTC), the National Telecommunications and Information Administration (NTIA), and the National Institute of Standards and Technology (NIST) are involved in these efforts. More than 200 organizations and individuals filed comments with NTIA last November, and these comments expressed broad support for federal privacy legislation. The stakes involved in consumer privacy legislation are high. Taking the wrong approach could have serious consequences for consumers, innovation, and competition. Moving forward with HB 457 would only complicate these efforts while ultimately consumer confusion.

In closing, there is no gap in privacy protections that need to be filled by HB 457. Consumers are well protected by the FTC, the nation's expert privacy protection

[9] *See* "Restoring Internet Freedom Final Order," *available at:* https://www.gpo.gov/fdsys/pkg/FR-2018-02-22/html/2018-03464.htm (Feb. 22, 2018).
[10] *See generally* Comments of CTIA, Developing the Administration's Approach to Consumer Privacy, NTIA Docket No. 180821780-8780-01 (Nov. 9, 2018).

enforcement agency. Accordingly, we would respectfully request that you table HB 457.

Thank you for the opportunity to testify today.