Testimony of
Gerard Keegan
CTIA

Before the Hawaii House of Representatives Committee on Consumer Protection & Commerce

February 13, 2018

On behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to Hawaii House Bill 2296 HD1, which would restrict how internet service providers (ISPs) operate in Hawaii.

Any suggestions that ISPs, including CTIA members, have unique access to consumer data online are unfounded. A comprehensive study by veteran Clinton and Obama Administration privacy expert Peter Swire showed that ISPs actually have limited insight into the online activity of consumers.[1] HB 2296 HD1 unnecessarily targets one set of providers - ISPs - and treats them differently than others operating in the internet ecosystem.

The wireless industry takes a proactive approach to protect consumer privacy. Our members provide consumers with detailed privacy policies, which clearly describe how providers protect consumer data. Current federal and state statutes also provide additional layers of protection for sensitive consumer information. In addition, ISPs, including CTIA members, have committed to principles that maintain privacy protections consistent with the Federal Trade Commission's effective privacy framework, covering transparency, consumer choice, security, and data breach notifications.[2]

CTIA member companies have long recognized the importance of protecting consumer data and respecting consumer privacy. In 2003, CTIA and the wireless carriers that are signatories to the "Consumer Code for Wireless Service," including AT&T, Sprint, T-Mobile, and Verizon Wireless, made a commitment to help consumers make informed choices.[3] The tenth point of the Code provides that signatory carriers agree to abide by policies for the protection of customer privacy. As part of that commitment, carriers follow policies regarding the privacy of customer information in accordance with applicable federal

[1] "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf, Swire, Peter, last accessed 2/12/2018: "ISP access to user data is not comprehensive – technological developments place substantial limits on ISPs' visibility. [And] ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs."
[2] "Protecting Consumer Privacy Online," http://www.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf, last accessed 2/12/2018.
[3] CTIA Consumer Code for Wireless Service, http://www.ctia.org/initiatives/voluntary-guidelines/consumer-code-for-wireless-service, last accessed 2/12/2018.

and state laws and make available privacy policies concerning information collected online. The wireless industry recognizes the importance of customer privacy and takes strong measures to protect customer data.

It is important to note that recent Congressional action did not change privacy protections for wireless consumers. The Federal Communications Commission (FCC) rules had not taken effect, so the 2017 CRA changed nothing from the regulatory framework that has existed since 2015.

Moreover, the FCC's recently adopted Internet Freedom Order means that the FTC will reassert its well-established oversight and enforcement authority over ISP consumer privacy practices.[4] 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. It is also consistent with the framework advocated for by the Obama Administration, which noted that, "uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers."[5] This legislation deviates from the privacy framework and standards that have been in place for decades and imposes unjustified restrictions on ISPs alone.

By creating two sets of rules that are different for various entities within the internet ecosystem, HB 2296 HD1 would harm competition and create consumer uncertainty about which rules apply to their data. Survey results submitted to the FCC last year showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules.[6] These findings indicate that HB 2296 HD1, which targets only ISPs, would in fact be a contravention to what consumers actually want. The bill would also make it very difficult – if not impossible - for ISPs to operate in Hawaii and could have a host of unintended consequences. Additionally, 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.

CTIA members are absolutely committed to protecting consumer information as they value consumer trust. Existing federal and state laws and protections remain intact today rendering HB 2296 HD1 unnecessary. Moreover, CTIA members have committed to a framework to protect consumer information and privacy. For these reasons, we respectfully ask that you not move HB 2296 HD1.

---

[4] *See* FCC Restoring Internet Freedom Report & Order ¶ 194 (adopted Dec. 14, 2017; issued Jan. 4, 2018), http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf.

[5] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc, last accessed 2/12/2018.

[6] The Progressive Policy Institute, "Consumers Want One Set of Rules Protecting Their Information," http://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/, last accessed 2/12/2018.