Testimony of
BENJAMIN ARON
CTIA

In Opposition to New Hampshire House Bill 1680 as amended

Before the
New Hampshire House Commerce and Consumer Affairs Committee

February 21, 2020

Chair, Vice-Chair, 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 1680 as amended. This bill would impose unworkable restrictions on how internet service providers (ISPs) manage customer-related information. If enacted into law, these restrictions would create serious unintended consequences that would harm New Hampshire businesses and consumers.

With the Federal Communications Commission’s Restoring Internet Freedom Order in effect, the Federal Trade Commission (FTC) once again has 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. The FTC is an active consumer privacy enforcer. It has brought over 500 enforcement actions protecting consumer privacy. Through these enforcement actions, as well as through extensive policy guidance, the FTC has articulated a consumer privacy framework in which more sensitive personal information (e.g., biometric or genetic information, children’s information, and health information) is generally subject to heightened protections, while there is greater flexibility to collect, use, and disclose non-sensitive information. The FTC is currently in the process of collecting extensive, detailed information from multiple ISPs for an industry-wide study into ISP privacy practices, ensuring the
FTC remains a well-educated and well-equipped consumer privacy enforcer.\textsuperscript{1} In addition, the New Hampshire Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under state consumer protection laws. Because of these existing federal and state measures, and other privacy laws, there is no gap in ISP customers’ privacy protections that New Hampshire needs to fill.

HB 1680 as amended 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.\textsuperscript{2} These findings indicate that state legislation, like HB 1680 as amended, targeting ISPs would in fact be inconsistent with what consumers actually want.

In addition, ISPs do not have unique access to consumer data. A study by noted 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 may have access to more information and a wider range of user information.\textsuperscript{3} Furthermore, consumers no longer use a single stationary device. Today consumers

\begin{itemize}
\item \textsuperscript{3} “Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,” \url{http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf}, Swire, Peter, last accessed 2/6/2020; “ISP access to user data is not comprehensive – technological developments place
use many connected devices serviced by multiple ISPs.

Moreover, research indicates that more than 80 percent of web traffic is encrypted, and that number continues to grow.\textsuperscript{4} Google estimates, for example, that 94 percent of traffic across Google is encrypted.\textsuperscript{5} 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.

Uniform federal policies work best. CTIA and its members support efforts to address the growing challenges to consumers’ privacy. In particular, CTIA supports federal legislation that establishes uniform, technology-neutral consumer privacy protections. Such legislation is the only way to ensure clearer, more specific, and nationally consistent privacy protections for consumers and certainty for businesses.

HB 1680 as amended would not produce any of the benefits of a uniform federal approach. To the contrary, it would create a highly restrictive technology-specific privacy regime. This legislation would require ISPs (but not other entities) to obtain “express affirmative consent” from consumers to use, disclose, sell or otherwise disseminate consumers’ personal information. Such a sweeping and inflexible opt-in requirement is at odds with nearly every other U.S. consumer privacy law and framework. As a result, this bill would change how New Hampshire consumers access information on the internet causing consumer confusion by creating different levels of privacy protections based on the type of entity that handles their personal information, 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.”


something consumers would not expect.

Maine passed an ISP-only privacy law last year. Last week, CTIA, along with other associations representing broadband providers, filed a lawsuit in the U.S. District Court of Maine. Maine’s decision to impose unique burdens on ISPs’ speech — while ignoring the online and offline businesses that have and use the very same information and for the same purposes as ISPs — represents discrimination between similarly situated speakers that is impermissible under the First Amendment.

In addition, the Maine law is preempted by federal law because it directly conflicts with federal determinations about the proper way to protect consumer privacy. Among other things, the law conflicts with the FCC’s decision that a combination of disclosure, competition, and FTC oversight — not prescriptive ISP-specific rules — best balances the federal policies of promoting broadband and protecting consumer privacy.

In closing, conflicting state rules could hamper the provision of broadband service in New Hampshire, lead to increase compliance costs, and inhibit providing new and innovative products and services — all to the detriment of consumers. Accordingly, CTIA respectfully requests that you not move this legislation as amended. Thank you for your consideration.