Testimony of
GERARD KEEGAN
CTIA

In Opposition to Massachusetts House Bill 382

Before the
Massachusetts Joint Committee on Economic Development and Emerging Technologies

October 22, 2019

Chairs, Vice-Chairs, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, I write in opposition to House Bill 382. This bill would impose unworkable restrictions on how internet service providers (ISPs) may collect, use, and disclose certain customer-related information. If enacted into law, these restrictions would create serious unintended consequences that would harm Massachusetts businesses and consumers.

Federal law provides robust privacy protection. Like nearly all other entities that handle U.S. consumers' personal information, ISPs are subject to the authority of the Federal Trade Commission (FTC). The FTC has brought over 500 privacy and data security cases against companies that have allegedly engaged in unfair or deceptive practices. 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. In addition, the Massachusetts Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under the Massachusetts 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

Massachusetts needs to fill.

Uniform federal policies work best. Nonetheless, 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.

H.382 would not produce any of these benefits of a uniform federal approach. To the contrary, it would create a highly restrictive state- and technology-specific privacy regime. The bill would require ISPs (but not other entities) to obtain "express written approval" from consumers to collect, use, disclose, 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 cause consumer confusion by creating different levels of privacy protection based on the type of entity that handles their personal information, something consumers would not expect.

By limiting ISPs' ability to communicate with consumers through a sweeping opt-in restriction, H.382 would burden ISPs' speech in a significant way. However, by limiting these restrictions to ISPs and not applying them to other entities within the "internet ecosystem," H.382 would likely violate the First Amendment. As leading constitutional law scholar Laurence Tribe has written, "singl[ing] out broadband ISPs for extremely burdensome regulation while ignoring the fact that much of the same information is available to and routinely used by social media companies, web browsers, search engines, data brokers, and other digital platforms" shows that the regulations "are not tailored to any

important government interest."[1] Accordingly, I respectfully urge you not to move this legislation.

[1] *See* Comments of Professor Laurence Tribe on FCC Broadband Privacy Regulations, available at https://ecfsapi.fcc.gov/file/60002079394.pdf and https://ecfsapi.fcc.gov/file/10913635001823/Supplemental%20White%20Paper%209-13-16.pdf, at 1.