



**Testimony of
GERARD KEEGAN
CTIA**

In Opposition to Connecticut Senate Bill 1108

March 25, 2019

**Before the
Connecticut Joint Government Administration and Elections Committee**

Co-chairs, vice-chairs, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, I submit this testimony in opposition to Senate Bill 1108, which would establish state regulations to address an inherently national and global issue: the protection of personal data. A law that sweeps too broadly, as SB 1108 does, will create security risks for consumers and presents serious compliance challenges for businesses.

SB 1108 creates broad access requirements that are in tension with data security principles, as they may encourage companies to centralize—rather than segregate—consumer data in one location, pool consumer data about particular requesting consumers in one location, and/or maintain consumer data in personally identifiable form, all to be able to comply with consumer requests. These practices inherently carry risks, such as making the data a more attractive target to identity thieves and cyber criminals. They can also be burdensome.

The deletion requirements in this legislation will be overly burdensome on companies. These requirements may also undermine important fraud prevention activities by allowing bad actors to suppress information. Moreover, these requirements may jeopardize the availability or quality of free or low-cost goods and services which are



exchanged for personal data. Often, consumers have access to free or low-cost goods or services because they allow a company to use their personal data. While consumers should always be provided meaningful notice and choice before their personal data is used, that choice should be balanced against the numerous benefits to consumers. Furthermore, the broad opt-out provisions in the bill, which allow consumers to say no to most data uses that are not essential to performing the contract, may introduce a host of unintended consequences. For example, consumers are accustomed to receiving news and other content for free in exchange for certain responsible uses of data. These opt-out provisions may fundamentally change how the internet operates in Connecticut.

Consumer privacy is an important issue. State-by-state regulation of consumer privacy will create an unworkable patchwork that will lead to consumer confusion. That is why CTIA strongly supports ongoing efforts within the federal government to develop a uniform national approach to consumer privacy.¹ 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 broad and sweeping state legislation would only complicate these

¹ See *generally* Comments of CTIA, Developing the Administration's Approach to Consumer Privacy, NTIA Docket No. 180821780-8780-01 (Nov. 9, 2018).



efforts while imposing serious compliance challenges on businesses and ultimately consumer confusion.

In closing, fragmented privacy approaches across states are difficult, and sometimes impossible, to effectively implement. Even the most well-intentioned companies will face steep hurdles attempting to comply with various, overlapping, and sometimes conflicting state laws. Connecticut should not enact complicated privacy legislation that creates security risks and raises the prospect of costly compliance for businesses operating in the states. For these reasons, CTIA opposes SB 1108.