Testimony of
GERARD KEEGAN
CTIA

In Opposition to Hawaii House Bill 2572 SD1

Before the
Hawaii Senate Committee on Commerce, Consumer Protection & Health and Committee on Technology

June 23, 2020

Chairs, Vice-Chairs, and committee members, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to House Bill 2572 SD1. Definitions in the bill are overly broad, and the legislation would have a host of unintended consequences.

The Federal Trade Commission's privacy framework considers precise geolocation information as sensitive information. CTIA supports the FTC framework but has concerns with the geolocation section of HB 2572 SD1. Data and artificial intelligence (AI) help providers look for indicators of fraudulent behavior. For instance, if a provider sees a consumer logging into an online account from Hawaii, but the consumer's cell phone is located in New Jersey, that alerts the provider to possible fraud. If a customer's login occurs from a Hawaii IP address, and the same customer's cell phone location recently registered in Hawaii, that is a sign the consumer is traveling. A provision requiring a possible wrongdoer in Hawaii to opt in to the "sale" of location information, which is broadly defined, could hamper a provider's ability to use location in this way to detect and prevent fraud.

Additionally, there are a number of smartphone apps designed for parents to monitor children, and these are generally based on the use of geolocation information. HB 2572 SD1 creates ambiguities for how these apps may function that raise serious concerns. Can children give consent or disable parental controls? Is parental consent sufficient, or could a child override the controls by not giving consent? HB

2572 SD1 could ultimately require a child to provide opt-in consent before a parent or guardian can initiate a tracking service or application. Finally, the definition of "geolocation information" is overly broad and will introduce a host of unintended consequences. For example, a consumer's zip code could be interpreted to fall under the definition of geolocation information, which is not the type of information that CTIA thinks the legislature intends to identify as geolocation information.

In closing, HB 2572 SD1 could hinder fraud prevention, hamper consumer use of certain applications, and prevent internet companies from providing new and innovative products and services – all to the detriment of consumers. As the pandemic is still upon us, CTIA respectfully urges the legislature to reject hastily drafted legislation like this bill that could have serious operational impacts and compliance costs. California is the only state to pass comprehensive privacy legislation, and that law comes with estimated initial compliance costs of $55 billion or 1.8% of the state's gross domestic product. Moreover, HB 2572 SD1 would only further fragment privacy regulation in the United States. This fragmentation does not benefit consumers. For these reasons, CTIA respectfully requests that you not move this legislation.