February 9, 2021

Oppose House Bill 1330
House Industry, Business and Labor
Chairman Mike Lefor

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee:

On behalf of CTIA®, the trade association for the wireless communications industry, I write to you in opposition to House Bill 1330. This bill raises particular concerns because its requirements would (1) clash with existing privacy protections, potentially creating consumer confusion, (2) mandate an onerous opt-in framework for the "sale" of "protected data"--concepts that are undefined or vague and/or overly broad, and (3) impose a significant compliance burden, particularly for small- and medium-sized companies. These concerns are even more alarming due to the enormous class action liabilities businesses could face under this bill. With per-user damages of up to $100,000 per violation, the class action provisions in this bill could bankrupt businesses.

The bill creates inconsistencies with existing legislation and protections, potentially resulting in consumer confusion and notice fatigue. Consumer privacy protections should be conceptually and operationally consistent. HB 1330 instead relies on new concepts and frameworks with little basis in existing privacy laws. Most importantly, the definition of "protected data" is not clearly limited to data that is personal in nature and therefore goes beyond existing privacy laws. For example, under the bill "a user's location" or "internet browsing history" could be considered protected data, even if the data would not be linkable to the underlying user, and even if it has been de-identified. The bill also contains no exclusion for data that is publicly available.

California is the only state to pass a comprehensive consumer privacy law. The CCPA provides an opt-out right for the sale of personal data. HB 1330 requires an opt-in right for North Dakota residents. For companies offering service in North Dakota and California, this would be burdensome and would be the start of an onerous patchwork of regulation across the country, and importantly would confuse consumers who would be confronted with overlapping and contradictory privacy protections as they interact with companies.

Users could also experience "notice fatigue" and simply approve every request without paying attention to how it affects their privacy rights. For example, if a consumer orders a new phone from a wireless provider, or any product from any retailer, it appears that the provider or retailer would need to get consent to share the consumer's address with the postal service or shipper to have the phone delivered. On the whole, the bill's consent requirements could lead

to “notice fatigue,” in which consumers stop paying attention to notices and simply click to approve every request – but businesses would still face the burden of presenting and recording these consents. The burden of complying with this kind of obligation would be tremendous, especially for smaller organizations, and would not provide corresponding consumer benefits.

Furthermore, the bill’s opt-in requirements are vague, overly broad and onerous, resulting in additional consumer confusion and generating potential inadvertent violations by businesses. HB 1330’s opt-in provision requires that companies provide users with the opportunity to opt-in to the “sale” of “protected data,” prohibiting companies from selling protected data “to another person” unless the user affirmatively opts-in. The term “sale” is not defined, and it is not clear whether the term would be limited to an exchange involving monetary consideration or whether companies’ routine sharing of data for a business purpose might inadvertently be swept in. For example, without a definition, the term “sale” could potentially include everyday transfers of information necessary for business purposes, such as the exchange of shipment information from a merchant to a mail carrier for fulfillment of consumer orders or the use of back-office cloud tools or platforms for purely internal purposes. Similarly, the bill’s framework could potentially cover the transmittal of location information from a ride sharing application to its drivers who are independent contractors.

Additionally, the term “person” is not defined, and it is not clear whether transfers of protected data between related or affiliated companies could be considered a sale. Without definitions for these terms, companies may reach widely varying conclusions regarding what the bill requires, resulting in inadvertent costly violations by businesses making good faith attempts to comply, as well as creating additional confusion for consumers.

The bill would impose significant compliance burdens, especially on small- and medium-sized businesses, with no evidence of benefit. Broad opt-in consent requirements provide little evident benefit to consumers and are burdensome, if not infeasible, for businesses to implement. This would be particularly true for HB 1330, which would theoretically apply in the same fashion to “protected data” no matter how it is collected – whether online, over the phone, or in person. For example, a call center could potentially be required to obtain opt-in consent for each “type” of protected data the call center collects in order to fulfill a consumer request, requiring call center agents to work through a significant and lengthy script to effectuate opt-in consent. As another example, physical retailers could be required to obtain opt-in consent from customers that walk into physical locations, requiring those retailers to develop a prescriptive compliance program for customer-facing staff that are responsible for collecting protected data.

HB 1330 differs from existing privacy regimes, some of which contain “thresholds” for application (e.g., annual gross revenue minimums, maintaining personal data from a

minimum number of consumers), by applying to businesses both small and large. In other words, a company with a single physical retail location and tens of thousands of dollars in revenue would be subject to the same compliance regime as a company with millions of dollars in revenue and dedicated privacy staff.

The lack of clarity in the bill will expose businesses making a good faith effort to comply to tremendous financial liability. The "penalties" provisions of the bill would impose unprecedented levels of potential liability on businesses and would be especially harmful for small and medium businesses. The bill would provide for statutory damages for violations of at least $10,000 for each user (plus reasonable attorneys' fees), or $100,000 for "knowing" violations (again, for each user). Given the lack of clarity in the bill, even businesses that make a good faith attempt to comply could face catastrophic penalties that could potentially force them to shut down. Businesses may consider such levels of liability and risk unacceptable and decline to start or continue doing business in North Dakota.

As mentioned, California is the only state to enact a comprehensive privacy law and it is still a moving target. It became effective Jan 1 2020; AG enforcement began July 1, 2020. Clarifying bills were passed by legislature in 2019 and 2020. And now with the passage of the ballot measure Prop 24 in November, the California Privacy Rights Act, (CPRA) further changes to the law are being made with new requirements effective in 2023. Accordingly, we caution North Dakota and any state from rushing to follow California down this unproven, untested, and unknown path. Protecting personal data is a national and global issue.

CTIA members are strongly committed to protecting the privacy of their customers, and CTIA supports uniform, technology-neutral consumer privacy protections. Federal legislation is the only way to ensure clear, consistent privacy protections for consumers and certainty for businesses. Neither consumers nor businesses benefit from the fragmentation that additional privacy laws at the state and local levels introduce. As such, CTIA opposes HB 1330 and respectfully urges the committee not to move this bill.

Sincerely,

Lisa McCabe
Director, State Legislative Affairs