February 9, 2021

Honorable Logan Phillips, Chair
Honorable Danny Williams, Vice Chair
Oklahoma House Technology Committee

Re: HB 1602 Opposition

Dear Chair Phillips, Vice Chair Williams and Committee Members:

On behalf of CTIA®, the trade association for the wireless communications industry, I write to you in opposition to House Bill 1602, 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 HB 1602 does, will create security risks and presents serious compliance challenges for businesses.

State legislation that sweeps too broadly could have a negative effect. HB 1602 has some commonalities with a California law that was hastily passed in 2018, without sufficient consultation with impacted stakeholders, and that contains many ambiguities. California is the only state to enact a comprehensive privacy law and it is still a moving target. It became effective January 1, 2020; Attorney General enforcement began July 1, 2020. Clarifying bills were passed by the legislature in 2019 and 2020. And now, with the passage of the ballot measure Prop 24 in November, the California Privacy Rights Act, further changes to the law are being made with new requirements effective in 2023. As such, the California law is a moving target, and attempts to follow California means that we will have the beginning of a patchwork of state laws that will confuse consumers and burden businesses. Oklahoma should not rush to follow California.

HB 1602 creates broad access requirements that are in tension with data security principles, as they may encourage companies to centralize—rather than segregate—customer data in one location, pool customer data about particular requesting consumers in one location, and/or maintain customer data in personally identifiable form, all to be able to comply with customer requests. These practices inherently carry risks, such as making the data a more attractive target to identity thieves and cybercriminals. They can also be burdensome. In the United Kingdom, a white hat hacker was able to get his fiancée’s credit card information, passwords, and identification numbers by making a false request. Similar scenarios will likely happen in California and in Oklahoma if the state enacts HB 1602.

It is also unclear how requirements to have consumers delete their data will turn out in practice. These requirements may undermine important fraud prevention activities by allowing bad actors to suppress information. Additionally, there is a concern that bad actors could request deletion of data that would flag them as wrongdoers. Businesses may also have to delete data that will help them track the quality of service to improve their products.

1 Leo Kelion, Black Hat: GDPR privacy law exploited to reveal personal data, BBC (August 8, 2019)
The stakes involved in consumer privacy legislation are high. Being too hasty to regulate could have serious consequences for consumers, innovation, and competition. Regulation can reduce the data that is available for research and for promising new solutions by putting too many constraints on the uses and flow of data. We are starting to see indications of this in Europe, where sweeping new privacy regulations took effect in 2018 and investment in EU technology ventures has declined. Similarly, the United States leads Europe in the development of Artificial Intelligence, and experts believe that Europe’s new data protection laws will increase this competitive disadvantage.

Any new state privacy law will contribute to a patchwork of regulation that will confuse consumers and burden businesses that operate in more than one state. Should the data of consumers who live in border cities and towns be treated differently when they cross the Oklahoma border? Should businesses with operations in multiple states segregate the data of Oklahoma citizens?

Much of the focus in the privacy debate thus far has been on compliance costs and the impact on larger companies, but regulation impacts business of all sizes. As part of the California Attorney General’s regulatory process, the office commissioned an economic impact study. The study found that the total cost of initial compliance with the law would be approximately $55 billion or 1.8% of the state’s gross domestic product.

In addition, the study found that any business that collects personal information from more than 137 consumers or devices a day would meet the law’s thresholds, while between 50 to 75% that earn less than $25 million in revenues will have to comply with the law. It also found that “[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.” These compliance costs include new business practices, operations and technology costs, training requirements, recordkeeping requirements, and other legal fees. It goes on to further state that “conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms … however evidence from the EU suggests that the opposite may be true.” The study found that many smaller firms have struggled to meet compliance costs. The EU regulation of privacy seems to have strengthened the position of the dominant online advertising companies, while a number

3 Daniel Castro and Eline Chivot, Want Europe to have the best AI? Reform the GDPR, IAPP Privacy Perspectives (May 23, 2019).
5 Id at 11.
6 Id at 11 and 20.
7 Id at 31.
8 Id at 31.
of smaller online services shut down rather than face compliance costs.

The scope of the law will likely impact smaller companies and firms. For example, a company or firm that may not meet the applicable thresholds may still be required to comply with the law if the company processes data for an entity that must comply. In that instance, an IT processing firm that processes consumer data for a larger business must be capable of responding to access and data deletion requests.

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. 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 federal efforts while imposing serious compliance challenges on businesses and ultimately confusing consumers. As we support a comprehensive federal privacy law, we oppose further fragmentation that would also arise from passage of HB 1602.

As mentioned, the only state to enact a comprehensive privacy law is California and it is still a moving target. It is simply not clear that we have found a good formula for regulating privacy. Accordingly, we caution Oklahoma and any state from rushing to follow California down this unproven, untested, and unknown path. As such, CTIA opposes HB 1602 and would urge the committee not to move this bill.

Sincerely,

Lisa V. McCabe
Director, State Legislative Affairs