Testimony of
LISA MCCABE
CTIA

Senate Bill 11

Before the
Maryland Senate Finance Committee
January 26, 2022

Chair Kelley, Vice Chair Feldman, and members of the committee, on behalf of CTIA®, the trade association for the wireless communications industry, thank you for the opportunity to provide this testimony on Senate Bill 11, which would establish state regulations to address an inherently national and global issue: the protection of personal data. A state law that sweeps too broadly, as these bills do, will create security risks and presents serious compliance challenges for businesses.

State legislation that sweeps too broadly could have a negative effect. This bill has some commonalities with a California privacy statute initially adopted in 2018, and exemplifies overly broad legislation that is difficult and costly to implement. Bills were passed by the California legislature in an attempt to clarify the statute in 2019 and again in 2020. Then a ballot measure – the California Privacy Rights Act – was passed in November 2020, which further changed the law, imposing new requirements effective 2023. And the statute called for implementing regulations, which have been voluminous, and additional regulations will follow as a result of the new requirements under the ballot measure. Even with the serial changes and extensive regulations, the scope of the statute remains broad and ambiguous, making

compliance difficult and expensive for business.

In 2021, Colorado and Virginia likewise passed comprehensive privacy laws that have yet to be implemented. We now truly have a patchwork of state laws that will confuse consumers and burden businesses. Maryland should not rush to follow other states down this path to the detriment of both consumers and businesses.

This bill, like the California statute, 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 consumers in one location, and/or maintain customer data in personally identifiable form, all to be able to comply with customer requests.

Requirements like the ones included in SB 11 put more burdens on companies in their efforts to prevent unauthorized access to data, which can be an attractive target to identity thieves and cybercriminals. 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.[1] Similar scenarios will likely happen in Maryland if the state enacts SB 11.

The practical implications of requirements permitting consumers to delete their data are unclear. These requirements may undermine important fraud prevention activities by allowing bad actors to suppress information. Businesses may also have to delete data that will

[1] Leo Kelion, Black Hat: GDPR privacy law exploited to reveal personal data, BBC (August 8, 2019).

help them track the quality of service to improve their products.

Moreover, the broad opt-out provisions in the bill may jeopardize the availability or quality of free or low-cost goods and services, which rely on the use of personal data that is subject to safeguards, such as pseudonymization. Online news sites, content providers, and apps are often provided to consumers free of charge because they are supported by advertising. These content providers should not be forced to continue to offer free services to consumers who opt-out of disclosing online identifiers to advertisers. 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.

While it is clear that these provisions create risk for consumers and cost for businesses, it is not clear that their benefits outweigh these risks. In Europe, consumers get reams and reams of data when they submit access requests, and they are constantly bombarded with pop-up windows as they browse the internet. Does this enhance their privacy or make their data more secure?

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.[2] 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.[3]

The broad privacy law in the E.U. has resulted in confusion for both small businesses and consumers. For example, a hairdresser refused to provide a customer with the brand and type of hair color used due concerns over data protection and a paramedic was denied the medical history of an unconscious patient over privacy law concerns.[4]

Additionally, in order to address some of the unintended consequences of broad privacy regulations, in the U.K., which has a statute similar to that in the E.U., the government recently signaled its intention, following Brexit, to revisit the U.K. General Data Protection Regulation (UK GDPR). The reforms in the U.K. are aimed at reducing barriers to innovation; reducing burdens on businesses and delivering better outcomes for people; boosting trade and reducing barriers to data flows; delivering better public services; and reform of the UK regulator, the Information Commissioner's Office.[5]

Any new state privacy law will contribute to a patchwork of regulation that will confuse

---

[2] Jia, Jian and Zhe Jin, Ginger and Wagman, Liad, "The Short-Run Effects of GDPR on Technology Venture" Investment, *National Bureau of Economic Research* (November 2018).
[3] Daniel Castro and Eline Chivot, Want Europe to have the best AI? Reform the GDPR, IAPP Privacy Perspectives (May 23, 2019).
[4] Hairdresser told customer she couldn't get details about hair dye due to 'GDPR concerns', Independent.ie, November 19, 2021
[5] Significant Changes Proposed to UK GDPR, JD Supra, (September 23, 2021).

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 Maryland border? Should businesses with operations in multiple states segregate the data of Maryland 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.[6] 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.[7]

The study further found that "[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.[8] 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."[9] The study found that many smaller firms have struggled to meet compliance costs. The EU regulation of privacy

---

[6] See Standardized Regulatory impact Assessment: California Consumer Privacy Act of 2018 Regulations, Berkeley Economic Advising and Research, LLC (August 2019).
[7] *Id* at 11.
[8] *Id* at 31.
[9] *Id* at 31.

seems to have strengthened the position of the dominant online advertising companies, while a number of smaller online services shut down rather than face compliance costs. SB 11 includes a threshold of applying to an entity that processes or maintains the personal information of 100,000 or more consumers, or devices during the course of a calendar year. This translates to just over 273 unique transactions per day, which would likely impact a small business in Maryland.

Consumer privacy is an important issue and the stakes involved in consumer privacy legislation are high. 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. Taking the wrong approach could have serious consequences for consumers, innovation, and competition in Maryland. 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 SB 11.

As mentioned, California is still a moving target and Virginia and Colorado have yet to implement their laws. It is simply not clear that we have found a good formula for regulating privacy. As such, CTIA opposes SB 11 and respectfully urges the committee not to move this bill.