Testimony of
LISA MCCABE
CTIA

In Opposition to Senate Bill 957

February 19, 2020

Before the
Maryland Senate Committee on Finance

Chairman Kelley, Vice Chairman Feldman, and members of the committee, on behalf of CTIA, the trade association for the wireless communications industry, thank you for the opportunity to testify in opposition to Senate Bill 957, 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 957 does, will create security risks and presents serious compliance challenges for businesses.

State legislation that sweeps too broadly could have a negative effect. SB 957 is based on a California law that was hastily passed in 2018, without sufficient consultation with impacted stakeholders, and that contains many ambiguities. California legislators enacted certain amendments last year – some with one-year sunsets to continue work in 2020 and 2021 – and may seek additional amendments to the law this year. The California Attorney General is also engaged in a rulemaking process to interpret its provisions. In addition, the sponsor of the original law is now proposing a ballot initiative to add further provisions to the law and change other provisions. 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. Maryland should not rush to follow California.

SB 957 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.[1] Similar scenarios will likely happen in California and in Maryland if the state enacts SB 957.

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.

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

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

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 as 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]

---

[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).

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 such as Ocean City or Chevy Chase 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.[4] 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.[5]

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.[6] It also found that "[s]mall firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.[7] 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

---

[4] See Standardized Regulatory impact Assessment: California Consumer Privacy Act of 2018 Regulations, Berkeley Economic Advising and Research, LLC (August 2019).
[5] *Id* at 11.
[6] *Id* at 11 and 20.
[7] *Id* at 31.

large technology firms … however evidence from the EU suggests that the opposite may be true."[8] 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 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 S957.

---

[8] *Id* at 31.

As mentioned, the only state to enact a comprehensive privacy law is California. This law took effect at the beginning of this year, and it is still a moving target: the legislature recently passed amendments, the Attorney General has yet to promulgate final regulations, and a new ballot initiative would make further substantive changes to the law. It is simply not clear that we have found a good formula for regulating privacy. Accordingly, we caution Maryland and any state from rushing to follow California down this unproven, untested, and unknown path. As such, CTIA opposed SB 957 and would urge the committee not to move this bill. Thank you for the opportunity to testify today.