STATE PRIVACY AND SECURITY COALITION

February 19, 2020

Senator Delores G. Kelley
Chair, Senate Finance Committee
3 East
Miller Senate Office Building
Annapolis, MD 21401

**Re: SB 957 (Oppose)**

Dear Chairwoman Kelley, Vice Chair Feldman, and Members of the Committee,

On behalf of the State Privacy and Security Coalition, a coalition of 30 leading technology, retail, communications, online security, payment card, and automobile companies, as well as eight trade associations, I appear today in opposition to SB 957.

Let me be clear: Our coalition believes that the federal government is the most appropriate venue for uniform privacy legislation. We understand, however, that state legislatures may be unwilling to wait for a federal solution. We are always willing to engage in a stakeholder process that would result in fair and meaningful privacy protections for consumers. We evaluate privacy legislation on whether it appropriately balances consumer control and transparency, operational workability, and cybersecurity (because as more information is provided to consumers, cybersecurity risks for all parties increases).

Unfortunately, this bill – based on the problematic California Consumer Privacy Act (CCPA) – does not meet these tests. In fact, it not only replicates problems that stem from the CCPA, it also creates new ones with the ways in which it strays from the CCPA. We discuss some of the most significant issues below.

## The CCPA is Not a Viable Model

It does not make sense to enact legislation in Maryland based on unfinished and confusing legislation like the CCPA.

Although part of the statute went into effect January 1, there are still significant changes likely to be implemented. First, the Attorney General's regulations are scheduled to be released sometime in the second quarter of 2020, with implementation beginning July 1, 2020. The initial draft was twenty-five pages of additional substantive requirements. The latest draft – released just last Friday – modified those requirements further, adding new requirements and deleting others.

Second, the original drafter of the 2017 CCPA ballot initiative has decided that he was unsatisfied with the ultimate outcome of CCPA, and consequently is gathering signatures to put forth another ballot initiative for 2020. This will significantly overhaul the current text of the statute, and create new, additional requirements.

Since its passage in June 2018, and including the two vehicles referenced above, the CCPA will have been amended *eight times* in just over two years. This is not the kind of sustainable, long-term vision that a state should apply to privacy law that governs cutting edge technology.

The CCPA's core aims – to provide consumers more transparency and control – can be accomplished with much simpler, much more comprehensible language that increases consumer benefit while reducing implementation costs.

**SB 957 Will Cost Millions of Dollars for Maryland's Small Businesses**

We recognize that SB 957 defines a "Business" with higher thresholds than the CCPA. Still, this would sweep in many small businesses in the state, saddling them with extreme compliance costs (particularly since SB 957 does not reflect the CCPA's amended definition of "Business" that removes reference to "devices"). A business that "collects" 100,000 pieces of personal information need only 274 transactions a day to be affected by CCPA – 274 unique visits to a website, or 274 credit card transactions for a merchant – and that business is within this legislation's scope.

The CCPA is incredibly and needlessly costly to the business community. The Attorney General's own study estimated that the cost of *initial* compliance costs for implementation would total $55 billion. For businesses with 20 or fewer employees, costs are estimated at $50,000. For businesses with fewer than 50 employees, costs are estimated at $100,000.

**SB 957 Would Eliminate Loyalty Programs for Maryland Consumers**

Unlike the CCPA, which contains some relief for businesses that offer loyalty and customer rewards programs, SB 957 would eliminate their use in the state, because the legislation would prohibit charging different prices or rates for goods or services, or providing a different level or quality of goods or services to the consumer. This is the core of many loyalty or frequent purchase programs, and would immediately mark Maryland as a stay-away for businesses that offer these types of programs.

**SB 957's Outlier Opt-Out Requirement Is Unworkable**

SB 957 goes far beyond the CCPA's already broad opt-out requirement for the "sale" of information. Even under the CCPA, the opt-out right is so far-reaching that it covers transactions like a business-to-business's website using a free analytics tool to understand the web traffic it is receiving. SB 957 goes much farther than this, purporting to benefit consumers by allowing an opt-out to any "disclosure" of information to a third party. In practice, this provision will be the subject of endless litigation and fails to recognize the realities of the online ecosystem.

The bill would create huge uncertainty over service provider and multi-party "ecosystem" arrangements by creating opt-out rights unless these disclosures were "necessary to the performance of a business purpose." Plaintiffs' lawyers and the AG's Office could challenge virtually any of these arrangements on the ground that it was not "necessary," even if it was

economically efficient and personal information was not used for any other purpose. This would be hugely disruptive with minimal if any benefit to consumers' privacy. Again, this goes far beyond the CCPA and it would make Maryland a more difficult state to do business in than any other state in a very important respect.

**SB 957 Does Not Reflect Many CCPA Amendments**

Even if SB 957 was enacted today, it would be out-of-date, because the CCPA has been amended in ways that do not accord with SB 957's current language. For example, critical definitions like "Business" were amended in October 2019 and are not reflected here.

Additionally, the CCPA added a minimal, but sensible and necessary, exemption for business-to-business data. Given that both CCPA and SB 957 purport to protect consumers and regulate consumer data, imposing additional requirements for business-to-business data seems illogical.

**SB 957 Creates Significant Cybersecurity Risks for Consumers and Businesses**

Like CCPA, SB 957 does not sufficiently allow businesses to take the possibility of fraud, and the maintenance of their cybersecurity infrastructure, into account when responding to consumer requests. Under this bill, a business would have to disclose the name of every cybersecurity vendor it uses, allowing hackers to use this law as a way of creating data maps to detect vulnerabilities. This alone is a multi-billion dollar risk for consumers' personal information.

Additionally, it applies a fraud exemption only to the Right to Delete. This means that if a fraudster impersonates a consumer (made easier by the lack of workable verification requirements in the bill), he or she can request *every piece of information* a business has on a consumer.

**SB 957's Enforcement Provisions Incentivize Litigation Over Pro-Privacy Practices**

The private right of action in this bill would eviscerate any progress that a privacy bill would accomplish. It has not been accepted in a single state that has seriously considered this type of legislation, including in the privacy laws recently passed in California and Nevada.

There are good reasons to reject class action enforcement. According to a study prepared by Hogan Lovells for the U.S. Chamber Institute for Legal Reform, plaintiffs rarely recover from lawsuits brought in privacy-related cases. Instead, this litigation "often leads to a major payday for plaintiffs' attorneys, even where class members experienced no concrete harm . . . even where class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation."[1]

[1] Mark Brennan et al., Ill-Suited: Private Rights of Action and Privacy Claims, U.S. Chamber Institute for Legal Reform at 5 (July 2019), available at: https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf

Private rights of action also open the door to class action lawsuits, which impose significant costs and do not result in meaningful benefits for consumers. One study[2] has shown that in over 150 federal class action lawsuits litigated in federal court: a) *not a single case* ended in a final judgment on the merits for the plaintiffs; b) 31% were dismissed by the courts on the merits; c) only 33% of the cases settled. When cases do settle, another study found that "the aggregate amount that class members typically receive comprises a small fraction of the nominal or stated settlement amount. Since courts base attorneys' fees on [this amount]…attorneys' fees often equate to 300%-400% of the actual aggregate class recovery."[3]

In conclusion, our coalition opposes SB 957. We would be more than willing to share our experiences as other states grapple with how best to protect consumers. In particular, we are part of the Oregon Attorney General's Privacy Task Force, and believe that process has been a productive method to bring various stakeholders to the table, and to systematically work through privacy issues at a granular level.

The issues involved here are technical and complex, with serious ramifications for both Maryland consumers and the business community. Accordingly, we ask that this committee not advance SB 957.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy and Security Coalition

[2] *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions* (2013), available at: https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf

[3] High Cost, Little Compensation, No harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes, Columbia Business Law Review (2017).