STATE PRIVACY AND SECURITY COALITION

March 25, 2019

Madame Chair Flexer, Chairman Fox, and Members of the Committee,

My name is Andrew Kingman, and I am counsel to the State Privacy & Security Coalition. We represent 23 companies and 6 trade associations in the communications, technology, retail, payment card, and online security sectors. I'm here today to speak in opposition to SB 1108, which is, as you know, almost entirely the text of the California Consumer Privacy Act (CCPA).

Unfortunately, the CCPA has fundamental and material flaws that this bill replicates. It is confusingly drafted, contains multiple internal contradictions, and this bill imposes an enforcement deadline that will likely be six months shorter than CCPA. In contrast, the European General Data Protection Regulations took 4 years to formulate, and gave 2 years to implement. This would give approximately 6 months of implementation time.

The CCPA's flaws can be seen in the attempted remediation. Following its passage, 20 democratic legislators sent a letter to leadership noting the need for legislative fixes. The Attorney General's office has requested a significant, additional appropriation for their office to help in both rulemaking and enforcement. And already this year, there are, at last count, 11 bills that are attempting to fix some portion of this legislation.

I. Key Points

- It does not make sense to introduce legislation in this state based on unfinished and confusing legislation from one other state.
- The definitions are so broad that they create significant unintended consequences that are neither pro-consumer nor pro-privacy, nor reflective of cybersecurity best practices.
- In key respects, the law would undermine privacy and data security. For example, the absence of a clear fraud exception would mean that hackers and other bad actors can require disclosure of information that jeopardizes other consumers' security.

II. The CCPA is still very much a Work in Progress

- CA Consumer Privacy Act (CCPA) is not ready for prime time.
- It was hastily and confusingly drafted, contains numerous ambiguities, and is likely to have significant negative unintended consequences for privacy.
- The law is a work in progress and by no means a model to pass in other states. The law will not take effect until Jan. 2020, is likely to be amended further, and will be clarified in Attorney General regulations. The effective date of the privacy provisions is not even set. It will take effect 6 months after publication of the final rules issued pursuant to the AG rulemaking or July 1, 2020, whichever is sooner.
- In short, we do not even know – and will not know for some time – what the CCPA will require once 2019 amendments and an Attorney General rulemaking are complete.

- The bill was introduced late night on Thursday, June 21 and was enacted in less than a week, leaving no room for the meaningful public consultation and stakeholder input that is critical for such far-reaching legislation.
- The sponsors acted in haste to avert an even more chaotic ballot initiative that was to be certified within days. That initiative would have required a super-majority of both houses of the legislature to modify.
- CCPA presents a hugely complex and technical set of issues that need to be studied and refined far more precisely than the CCPA does. There are major problems with the CCPA text (some of which are explained in Sections III and IV below). Trying to adopt this statute in Connecticut would create serious unintended consequences and harms both for privacy and for the state's economy that could last for decades.
- Legislation should not be introduced until we understand what the final requirements of the CCPA are, and if a clearer approach can achieve better privacy progress in a simpler way.

III. Unintended Negative Privacy Consequences

- Strongly incentivizes the combination and storage of all personal information a company holds in one place to be able to comply with consumer rights requests, thereby also increasing vulnerability to hacking and fraud.
- Because consumer data and consumer rights apply to a household as well as to an individual consumer, as drafted, an abusive spouse can request all PI on his or her victim, and roommates can obtain financial account and social security number information about other roommates; CCPA consumer rights also apply to employee data, meaning an employee fired for sexual harassment, fraud, theft, etc. can require the company to provide, and ask the company to delete, the record of their criminal data.

IV. Prominent Definitional Problems

- "**Personal Information**" – goes far beyond any other U.S. state or federal definition of personal information and is overbroad to the point of being meaningless. It covers all information that not only is "capable of being associated with", but also that simply "relates to" or "describes," an individual, device or household, even if that individual or household are not identifiable. It also can be read to encompass information that has been and remains de-identified, but is simply capable of being associated with a household.
    - The definition includes (but is not limited to): IP address, thermal information, olfactory information, employment-related information.
    - The overbroad, unnecessary scope of covered data does not enhance consumers' privacy protection, because it covers data having no relation to privacy rights. It would force businesses to associate truly identifiable data with otherwise non-

identifiable data, thereby undermining existing privacy-protective business practices.

.

- "**Deidentified Data**" – Poorly Defined & Creates Risk for Consumer Privacy
  - Because the de-identified definition includes the phrase "does not…relate to, describe" an individual, it effectively includes only aggregate data
  - A well-crafted de-identified data definition should acknowledge that companies may hold information that relates to a specific consumer, but have no idea who the specific consumer is. For example, a company may know that the consumer is a female, or a customer enjoys surfing, but may not know anything else about him/her.
    - Similarly, a business might know that Person 123456 often buys blue pants from their online store, and where their encrypted payment information is stored. However, they do not know who Person 123456 is, and never tries to find this out.
  - De-identification is a privacy and cybersecurity good practice that should be encouraged, not defined out of existence.
    - De-identification exceptions are is pro-privacy and pro-security because they encourage businesses to keep different data in separate "buckets," which enhances privacy and limits the damage hackers can do. In sharp contrast, the CCPA strongly encourages businesses to pool all of their data in a single bucket to be able to comply with requests regarding bits and pieces of the huge range of "personal data."

- "**Sell**," "selling," "sale," or "sold," includes activities that are not sales.
  - The definition includes "disseminating, making available…or otherwise communicating orally…a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."
  - The definition is drafted so broadly that it reaches the provision of almost any paid service that simply transmits data to another party even if the receiving party does not pay the disclosing party anything, does not take ownership of the transmitted data, and is contractually prohibited from using the data for its own commercial purposes.
  - This definition, coupled with that of "Personal Information," is so broad that it reaches the provision of almost any paid service that simply transmits data.
  - What is more the CCPA imposes liabilities on businesses who fail to tell consumers they are selling their PI when, in fact, they are doing no such thing.

- **"Consumer" –** Includes all California residents, including when they are not consumers
  - This is a source of major confusion, because the law refers throughout to consumers, when it means .

- As drafted, an employee accused of sexual harassment could request that complaints about him or her be expunged from company files, and the company may believe it must comply—either because it misunderstands the complex provisions of the law or because it has not yet been made aware of the allegations of misconduct.

V. Prominent Operational Problems

Here is a small sample of other significant operational problems of the CCPA:

- **Insufficient Fraud Exemption**: The CCPA does not prevent bad actors from, for example, requesting deletion of their personal information from a company's systems that is necessary to thwart fraud or cyber attacks, or from obtaining key information about a business' fraud detection vendors.
- **Expanding Cybersecurity Vulnerabilities:** The CCPA currently requires companies to disclose to hackers the security vendors to which a company gives IP address and other potential threat information, which educates hackers regarding the company's cybersecurity capabilities and helps in planning cyber attacks. Additionally, the statute allows third parties to make opt-out requests on behalf of consumers, creating additional security risks.
- **Notice Fatigue: The definition of "homepage"** combined with the notice requirements of the bill and definition of either an IP address or a device ID as personal information, require a business to place privacy notices on every single webpage on its website, instead of just its actual homepage or a dedicated section on privacy.
- **Confusing Scope:** Also, although entitled a "consumer privacy act", the CCPA in fact appears to apply both to employee and to business-to-business data in ways that make no sense. It is also unclear whether the CCPA is applicable to businesses with >$25M in global or in-state revenue – a distinction with huge practical implications for small businesses.
- **Service Provider:** Currently, a service provider that receives consumer information from the business with which it has a contract is defined as "collecting" consumer PI, so that service providers confusingly most respond to consumer rights requests, instead of the business the state resident has a relationship with. That business should field the request and instruct the vendor to remove or port the data. The CCPA language does not make sense in the modern business context.

VI. In Short:

- The CCPA was **hastily and sloppily drafted** and enacted. It is **not ready for prime time**.
- The CCPA includes provisions that have the unintended consequence of **weakening consumer privacy** and **increasing security threats**, when sensible privacy legislation should do the opposite.

- The CCPA suffers from **numerous definitional and operational problems** that make implementation and compliance needlessly confusing for consumers and businesses alike and needlessly costly.
- CCPA would impose millions of dollars of compliance costs on most businesses and would **harm the state's economy** more than it would protect consumer privacy.
- Legislation should not be introduced until legislators, legal privacy experts representing consumers and businesses, and other stakeholders understand what the final requirements of the CCPA are, and whether a clearer, simpler approach can achieve better privacy protections without impairing the state's economy.

Thank you for your consideration. I would be happy to answer any questions.

Respectfully,

Andrew A. Kingman
Counsel
State Privacy & Security Coalition