December 2, 2019

Hon. Xavier Becerra
Attorney General
1300 I Street, 17th Floor
Sacramento, California 95814

Attention: Ms. Anabel Renteria
Initiative Coordinator

Dear Attorney General Becerra:

Pursuant to Elections Code 9005, we have reviewed the proposed statutory initiative related to consumer privacy (A.G. File No. 19-0021, Amendment #1).

Background

Businesses Collect and Use Consumer Data. Businesses primarily collect consumer data from (1) public sources, (2) consumers directly (such as when an individual creates an account or uses a product or service), or (3) other businesses (such as by purchasing the data). Businesses use this data for their own internal purposes, such as to improve sales or customer service. Businesses can also use this data to provide services to other businesses, such as Internet companies that target ads for other businesses using data collected from free services that the Internet companies provide to consumers. In using consumer data, businesses sometimes apply statistical formulas to various pieces of data to make predictions about consumer attitudes or preferences (such as lifestyle habits).

Consumer Data Privacy Requirements. Under state law, certain businesses (including their contractors and service providers) that operate in California and collect personal information from consumers must follow specific requirements surrounding consumer privacy, most of which go into effect January 1, 2020 or later. (Under state law, personal information generally includes various categories of information such as: name, social security number, purchase or Internet activity, location data, and predictions about consumers based on their data.) Generally, these are businesses that (1) earn more than $25 million in annual revenue; (2) buy, sell, or share the personal information of 50,000 or more consumers, households, or devices annually; or (3) earn 50 percent or more of their annual revenues from selling consumers' personal information. Businesses that control or are controlled by a business that meet any of the above thresholds, as well as share a common name or trademark with that business, must also comply with consumer data privacy requirements.

The specific consumer data privacy requirements that the above businesses must meet include:

- ***Notifying Consumers of Privacy Rights and Data Collection and Usage.*** Businesses generally must notify consumers if they collect or sell consumer personal information, as well as of the purposes for which the information will be used. Businesses must also notify consumers of their privacy rights related to their data, such as their ability to request and delete their personal information.
- ***Providing Consumers With Rights Related to Their Personal Information.*** Businesses must provide consumers with the right to request reports on personal information that is collected or sold at no charge to the consumer, generally within 45 days of being requested. Consumers can also direct a business to delete collected personal information, except in certain limited situations. In addition, consumers can direct a business to not sell their personal information.
- ***Providing Same Prices and Services to Consumers Who Exercise Their Rights.*** Businesses are prohibited from treating consumers who request reports on the use of their personal information or who direct businesses to not sell their personal information differently than other consumers. For example, businesses cannot charge consumers different prices for goods or services or provide them different levels of service or quality of products based on whether they exercise their personal information rights. Businesses, however, can offer financial incentives for the collection or sale of personal information.

Failure to comply with these requirements can result in penalties of no more than $2,500 for each violation or $7,500 for each intentional violation. These penalties only may be applied if businesses fail to address any alleged violation within 30 days of being notified. These penalties can only be sought by the Department of Justice (DOJ).

Data Breach Requirements. A data breach occurs when people gain unauthorized access to information, such as consumer data. State law requires that businesses take reasonable steps to protect consumer data from breaches, as well as notify people if their information was accessed in a data breach. Data breaches of certain personal information can result in penalties of $100 to $750 per consumer per incident or actual damages—whichever is greater. These penalties can be sought by DOJ or a consumer after a business fails to address any violation within 30 days of being notified.

Enforcement of Consumer Privacy and Data Breach Laws. DOJ currently oversees compliance with and enforces the state's consumer data privacy laws. For example, DOJ is responsible for ensuring compliance by addressing questions from businesses seeking guidance on how to comply with the state's data privacy requirements, as well as by developing regulations—such as rules for how businesses must process consumer requests to not sell their personal information. DOJ can enforce consumer privacy laws by prosecuting crimes (such as identity theft) or filing lawsuits in state trial courts against businesses who break these laws. Existing law generally requires that penalties assessed for violations of consumer privacy and certain data breach requirements be deposited into a state fund—the Consumer Privacy Fund

(CPF)—to offset trial court and DOJ costs related to these laws. If there is more funding than needed to fully offset these costs, the Legislature can allocate the remaining funds to other purposes.

Proposal

This measure (1) modifies existing consumer data privacy laws, (2) establishes new consumer privacy rights, (3) changes existing penalties and uses of penalty revenues, and (4) creates a new state agency to monitor compliance and enforcement of the state's consumer data privacy laws. If approved by the voters, most of the measure's provisions would take effect in January 2023 and would apply to data collected on or after January 2022. Select provisions (such as the creation of the agency and requirements for developing new regulations) would go into effect following voter approval.

Modifies Existing Consumer Data Privacy Laws. This measure changes which businesses are required to comply with state consumer data privacy requirements. For example, under current law, businesses that buy, sell, or share the personal information of 50,000 or more consumers, households, or devices annually are subject to consumer data privacy requirements. Under the measure, this threshold would increase to 100,000 or more consumers or households, with devices not counting towards the threshold. The measure also requires businesses that earn 50 percent or more of their annual revenues from sharing consumers' personal information comply with these requirements. (Currently, sharing is not specifically defined in state law. Under the measure, sharing is specifically defined as providing data for the purpose of targeted advertising based on consumers' personal information obtained from their activity across multiple businesses or websites.) Finally, the measure specifies that, generally, only businesses who control the collection of information—not their contractors or service providers—are subject to these requirements.

In addition, the measure requires businesses to apply existing consumer data privacy requirements to the sharing of personal information. For example, businesses must notify consumers if they share consumer personal information. The measure requires businesses to notify consumers of the length of time they intend to retain the various categories of personal information they collect about consumers.

Establishes New Consumer Privacy Rights This measure provides consumers with new consumer privacy rights with respect to businesses covered by this measure. These include the right to:

- ***Limit Sharing of Personal Information.*** Consumers could direct businesses to not share their personal information.
- ***Correct Personal Information.*** Consumers could request businesses to correct inaccurate personal information maintained about them, generally within 45 days of receiving their request. However, businesses are not required to do so if it was impossible or required disproportionate effort.

- ***Limit Use of Sensitive Personal Information.*** This measure allows consumers to direct businesses to limit the use of their sensitive personal information only to (1) provide services or goods requested by the consumer and (2) fulfill core business purposes (such as providing customer service). The measure defines sensitive personal information as specific pieces of personal information that are not publically available and reveals certain characteristics about the consumer. This includes social security numbers, account log-ins with passwords, and information collected and analyzed about the consumer's health.

Changes Existing Penalties and Uses of Penalty Revenues. This measure authorizes a penalty of $7,500 for violations of the consumer privacy rights of minors. The measure also eliminates the ability of businesses to avoid penalties by resolving violations within 30 days of being notified. In addition, the measure makes data breaches of email addresses, in combination with information that would permit access to an account (such as a password), subject to penalties. Additionally, it specifies that businesses would no longer be able to avoid penalties if they implement and maintain reasonable security procedures and practices to address a data breach within 30 days of the breach.

In addition, the measure limits the ability for the Legislature to use penalty revenue deposited into the CPF for purposes other than consumer privacy. Under the measure, each fiscal year after offsetting the state court and DOJ costs, 91 percent of remaining funds would be invested by the State Treasurer with any interest or earnings transferred to the state General Fund. The remaining 9 percent of funds would support nonprofit organizations educating the public on consumer privacy and law enforcement agencies combating fraud resulting from data breaches.

Creates New State Agency for Enforcement. This measure creates a new state agency, the California Privacy Protection Agency (CPPA), as the primary entity to monitor compliance and enforcement of the state's consumer privacy laws. The CPPA would be governed by a five-member appointed board and have a wide range of responsibilities. For example, the agency would be responsible for (1) investigating and adjudicating potential violations, (2) assessing penalties for violations, (3) developing regulations, (4) providing guidance to businesses and consumers, and (5) monitoring developments related to the protection of personal information. Despite the shift of enforcement responsibility to this new agency, DOJ would still be able, at its discretion, to pursue enforcement actions. Under the measure, DOJ enforcement action would generally have priority over those of the agency. Any decision by CPPA related to a violation complaint or assessed penalty would be subject to review by the state trial courts. This measure would appropriate $10 million annually (adjusted for cost-of-living changes) from the state General Fund to support CPPA's operations.

Other Provisions. The measure includes various other provisions related to privacy rights and requirements. For example, the measure requires DOJ and CPPA to develop a wide range of regulations—including rules for establishing the process governing consumer requests to correct data, as well as for determining which businesses would be required to conduct a risk assessment of their ability to protect privacy. The measure also exempts businesses from complying with certain consumer privacy requirements under specified conditions. For example, businesses

could refuse to delete data related to education assessments and could preserve data for law enforcement investigation purposes to comply with a court order.

Fiscal Effects

As we discuss below, the measure would impact both state costs and state and local tax revenues. The actual magnitude of these effects, however, are uncertain and would depend primarily on how consumers, businesses, and state and local government respond to its provisions. For example, it is unclear how affected businesses would change their operations and how may violations of this measure would be investigated and adjudicated.

CPPA Costs. As discussed above, the measure appropriates $10 million annually (adjusted for cost-of-living changes) from the General Fund for CPPA's operations. Depending on how the agency carries out its responsibilities to monitor compliance and enforcement consumer privacy laws, it is possible that CPPA's actual workload costs could be higher.

DOJ and Court Costs. This measure would impact both the DOJ and state court workload. The DOJ workload could increase if it chooses to investigate and/or file cases against businesses that fail to comply with the measure's new consumer data privacy requirements. However, this increased workload could potentially be partially or fully offset by reductions in workload from the measure shifting responsibilities from DOJ to CPPA. Additionally, state court workload could increase if the measure results in the filing of (1) lawsuits by DOJ for violations of the new requirements of this measure, (2) requests for review of CPPA complaint and penalty decisions, and (3) requests for the courts to enforce the collection of CPPA administrative penalties. The costs of this increased workload would depend primarily on the number of violations investigated and adjudicated, as well as the number and types of cases filed with the state courts. In total, increased state costs to DOJ and trial courts could reach the low millions of dollars annually. Some or all of these costs would be offset by increased revenue related to penalties assessed and collected from businesses violating consumer privacy laws.

Tax Revenues. The measure would have various impacts on businesses and consumers, which could then impact state and local tax revenues. On the one hand, the measure could reduce tax revenues in certain areas. For example, the measure's requirements could increase business costs, such as requiring new resources to address consumer requests to correct personal information. This could result in fewer taxes being paid by businesses to state and local governments. On the other hand, the measure could increase tax revenues in certain areas. For example, to the extent that the requirements reduce the severity or number of data breaches, the amount of money businesses and consumers lose due to such breaches would decline. This could increase tax revenues if consumers then spend more on taxable items and/or businesses earn more revenue. The overall net impact on the economy and state and local tax revenue is unknown and would depend on how businesses and consumers respond to the measure.

Summary of Fiscal Effects. The measure would have the following major fiscal effects:

- Increased annual state costs of roughly $10 million for a new state agency to monitor compliance and enforcement of consumer privacy laws.

- Increased state costs, potentially reaching the low millions of dollars annually, from increased workload to DOJ and the state courts, some or all of which would be offset by penalty revenues.
- Unknown impact on state and local tax revenues due to economic effects resulting from new requirements on businesses to protect consumer information.

Sincerely,

_____
Gabriel Petek
Legislative Analyst

_____
Keely Martin Bosler
Director of Finance