October 23, 2017

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

Attention: Ms. Ashley Johansson
Initiative Coordinator

Dear Attorney General Becerra:

Pursuant to Elections Code Section 9005, we have reviewed the proposed statutory initiative (A.G. File No. 17-0027, Amendment #1) relating to consumer privacy.

Background

Commercial Uses of Personal Information. Many businesses maintain a wide array of personal information on consumers, including their contact information, demographic background, financial activity, Internet history, physical characteristics (biometric data), and location. Businesses involved in the commercial use of consumer information—particularly data brokers—aggregate consumer data from multiple sources and then use the data for their own internal purposes and/or sell or share the information with other businesses. While the commercial use of personal information is the primary purpose of some businesses (such as data brokers), other businesses (such as retailers) engage in it as a secondary activity. For example, retailors will often use the personal information they collect to improve their marketing efforts and, in some cases, sell such information to third party businesses to use for their marketing efforts. Some businesses are heavily reliant on the collection and commercial use of consumer information to generate revenue, such as Internet companies that do not charge users for their services or data brokers that are focused on selling information to third parties.

Data Breaches. In a data breach, unauthorized individuals gain access to or control of data, such as personal information. Data breaches are generally carried out by criminals who seek to profit from the information—such as by using it in identity theft schemes. Between 2012 and 2016, the California Attorney General received reports of 657 data breaches affecting over 49 million records in California. Most data breaches in California occurred in the retail, financial, and healthcare sectors of the economy.

State and Federal Privacy Laws. The State Constitution guarantees individuals the right to privacy. State and federal law also include various other provisions related to privacy. Such provisions include:

- ***Information Sharing Limitations.*** State and federal law limit the types of personal information private entities can share with others. For example, state law requires banks to obtain a customers' permission before sharing their financial information. Similarly, federal law prohibits health care providers from sharing a patient's medical information without permission.
- ***Privacy Policy Requirements.*** State law requires Internet companies that collect personal information to clearly state their privacy policy on their website, including a description of what information is collected and the types of entities that the information is shared with.
- ***Information Disclosure Requirements.*** State law requires businesses that collect and share personal information about consumers for marketing purposes disclose—upon a consumer's request—the categories of information generally collected and shared and who it is shared with. In addition, federal law requires online services directed to children to provide notice of what information is collected from children and how it is used. These entities must also obtain parental consent for the collection, use, or disclosure of such information.
- ***Data Security Requirements.*** State law requires that a business that possesses consumer information to take "reasonable security procedures and practices" to safeguard that information from data breaches. The business must also require third parties that it shares personal information with to implement similar safeguards. In addition, the business must notify individuals if a data breach affects information about them.

Enforcement of Privacy Laws. The California Attorney General can enforce privacy laws by prosecuting crimes (such as identity theft and criminal invasion of privacy) and by bringing civil lawsuits against entities that violate privacy laws. In addition, individuals can bring their own lawsuits against private entities that unlawfully share their information or negligently fail to protect it from unintended breaches. In such cases, individuals must prove that they suffered harm (such as financial loss) as a result of the privacy violation.

Proposal

This measure places various requirements on businesses that collect, buy, or share personal information for commercial purposes. Specifically, the measure applies to those businesses that: (1) have annual gross revenues of $25 million or more; (2) derive at least 50 percent of their revenues from selling personal information; or (3) buy, receive, or share for commercial purposes the personal information of 50,000 consumers or more annually. The measure defines personal information to include (1) certain demographic data (such as race and gender), (2) unique identifiers (such as social security numbers and customer identification numbers), (3) biometric data, and (4) inferences drawn about customers from such data.

Requires Disclosure of Commercial Sharing of Personal Information. This measure requires that businesses notify consumers if they collect or share personal information for commercial purposes, as well as the categories of information collected. Businesses must also identify the third parties they provide such information to, as well as the third parties they buy information from and the categories of information involved. In addition, if requested by a

consumer, businesses must provide the above information as it pertains specifically to that consumer for the last 12 months. The measure prohibits any business from charging consumers who request the disclosure of such information different prices for the same service, or providing them with different levels of service.

Allows Consumers to Not Have Personal Information Shared. The measure generally allows consumers to "opt out" from allowing businesses to share their personal information for commercial purposes. Specifically, businesses would be required to notify consumers of their ability to opt out both on their websites and physical premises and provide customers with a way to opt out. The measure prohibits businesses from charging consumers who choose to opt out different prices for the same service, or providing them with different levels of service.

Establishes Liability for Data Breaches. The measure states that businesses would be subject to civil penalties (described below) if they experience a data breach involving consumers' personal information due to gross negligence. The measure defines gross negligence as a failure to use reasonable diligence to maintain the security of personal information given the available technology and the standard security practices of similar businesses.

Establishes Process to Enforce the Measure. Under this measure, consumers who have suffered a violation (such as having their information sold despite opting out or being the victim of a data breach) would be able to bring legal action against the involved business for statutory damages. Consumers would not have to prove that they suffered harm as a result of the violation to be awarded damages. The measure assigns statutory damages as the greater of $1,000 or actual damages for each violation by a business. In the case of knowing or willful violations, statutory damages would be between $1,000 and $3,000 or actual damages, whichever is greater.

Businesses that violate this measure would also be subject to civil action brought by the California Attorney General or local prosecutors (such as county district attorneys). The measure assigns civil penalties of up to $7,500 per violation for intentional violations. In addition, any "whistleblower" with non-public information that a business has violated the measure may request that the Attorney General file a civil action. If the Attorney General declines to do so, the whistleblower may file suit in place of the Attorney General.

Creates the Consumer Privacy Fund. Of the funding collected in civil penalties from civil actions brought by the Attorney General or local prosecutors, 20 percent would be deposited in a new state fund, the Consumer Privacy Fund (CPF). The remaining 80 percent would go to the jurisdiction the action was brought on behalf of, such as the state or county, which could be used to offset the jurisdiction's costs. If the civil penalties resulted from civil actions involving a whistleblower, a higher percentage of the funding collected would be deposited in the CPF, depending on the circumstances. Monies in the fund would be used to offset costs incurred by the state courts and the California Attorney General related to the measure. The Legislature could adjust the above percentages to help ensure state costs related to the measure are offset.

Requires California Attorney General to Adopt Regulations. The measure requires the California Attorney General to develop various implementation regulations, such as regulations governing how businesses must allow consumers to opt out. The Attorney General could also adopt other regulations—such as expanding the categories of personal information subject to the measure.

Fiscal Effects

State and Local Enforcement and Implementation Costs. To the extent this measure leads to more or lengthier civil actions against businesses, there would be additional workload for state courts. In addition, the California Attorney General's office and local governments would experience increased workload to the extent they brought civil actions related to the measure's provisions. The Attorney General would also have increased workload to develop the required implementation regulations. The costs of the above workload would depend on the number and type of cases filed, but could reach the low tens of millions of dollars annually. Some or all of these costs would be offset by increased penalty revenue resulting from the new civil penalties authorized by the measure.

Potential Tax Revenue Impacts. The measure would impose significant new requirements on affected businesses operating in California. These requirements to improve the privacy of consumer information would both raise the costs and reduce revenues of those businesses. The magnitude of these potential impacts on tax revenue are unknown and would depend on how the state and local governments, businesses, and the public responded to the measure.

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

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

Sincerely,

_____

Mac Taylor
Legislative Analyst

_____

Michael Cohen
Director of Finance