February 21, 2014

Hon. Kamala D. Harris
Attorney General
1300 I Street, 17th Floor
Sacramento, California 95814

Attention: Ms. Ashley Johansson
Initiative Coordinator

Dear Attorney General Harris:

Pursuant to Elections Code Section 9005, we have reviewed the proposed statutory initiative related to the online collection and use of personal information (A.G. File No. 14-0006).

Background

Personal Information Accessible to Online Entities. Once individuals connect to the Internet, their personal information is accessible to various online entities, such as the companies that make the web browsers individuals typically use to access the Internet. In some cases, the information is provided directly to an online entity by an individual. While in other cases, the information is collected by an entity without an individual actively providing it. For example, any text typed on a website can be scanned and read by online service and webpage providers, including search terms, addresses, login names and passwords, and e-mails. Additionally, in order to connect to the Internet, a computer needs an Internet Protocol (IP) address, which is a numerical label that identifies the computer when connecting to the Internet. Although the IP address does not specifically contain personal information identifying the user of the computer, it can report the location of the computer. We note that an IP address can be used by online service providers to track the activity and information provided online by the user of that computer, such as which websites the user visited.

Individuals who connect to the Internet with their smart phones also make their personal information accessible when using mobile applications. This is because such applications often require individuals to provide access to their personal information before they can install the applications. This includes access to phone and email contacts, Internet data, the smart phone's unique identifiers, how the application is used, and the phone's geographic location.

Online Entities Mainly Use Personal Information for Marketing. The majority of personal information tracked and collected by online entities is used for marketing, as well as assessing how individuals use websites. For example, websites often want the personal information of Internet users to help them attract new customers, retain old customers, and increase the amount of time customers spend on their site. Similarly, online advertisement companies use search

terms, demographic information, and online purchase history to tailor advertisements, advertisement placement, and products for target audiences. For example, if an individual starts spending time on websites with pregnancy information, that individual might start seeing more advertisements on their web browser for baby clothing.

Internet Users Have Some Tools to Increase Privacy. To some extent, individuals can control what personal information is collected about them while on the Internet. For example, most major web browsers offer "private browsing" tools to increase privacy and, thus, reduce the amount of personal information that can be accessed by online entities. These tools can include mechanisms to block devices that seek to track the personal information of an individual on the Internet, as well as a "Do Not Track" (DNT) setting that sends a signal to websites and online operators that the individual does not want to be tracked. While this setting is typically recognized by online service providers, there is no legal requirement that such providers adhere to it.

We also note that when individuals use "cloud computing," their ability to control the amount of personal information accessible by online entities is limited. (Cloud computing involves computers or drives operating as data storage centers connected through a network, such as the Internet, rather than on the individual's own computer, so that the individual can connect to other computers to store data and later access that data from any device connected to the same network.) This is because data stored on cloud drives can be read by the online service storing the data and its affiliates, and the data can sometimes be accessed illegally online by other entities.

State and Federal Privacy Laws. The State Constitution guarantees individuals the right to privacy. In addition, state and federal statutes place limits on the types of personal information that governments and private entities can disclose to others. For example, the Department of Motor Vehicles generally may not release an individual's residence address. State law also requires banks to obtain a customer's permission before sharing his or her financial information with other companies. Similarly, federal law prohibits health care providers from sharing a patient's medical information without permission.

State law requires all operators of commercial websites and online services that collect personally identifiable information to clearly state their privacy policy on their website. The policy must specify (1) all personal information that is collected, (2) the types of entities the information may be shared with, and (3) how the website or online service responds to a DNT signal that is received. Currently, the courts have interpreted this law to require compliance from both in-state and out-of-state organizations. Federal law requires website operators and online services directed to children to provide notice of what personal 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.

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 governments and private entities that unlawfully share their personal information or negligently fail to protect it from unintended breaches. In order for such a lawsuit

to succeed, a person must prove that he or she suffered harm (such as financial loss or emotional distress) as a result of the privacy violation.

Proposal

Classifies Certain Online Entities. This measure classifies certain online entities as first-party or third-party online services. According to the measure, a first-party online service is a service that individuals intentionally interact with, as well as any service that is owned and controlled by, and shares common branding with the service that the individual is interacting with. For example, an online store that an individual purchases products from is considered a first-party online service. The measure also states that a contractor hired by a first-party online service to provide certain services is also considered a first-party online service, if the contractor: (1) acts only as an information processor on behalf of the first-party online service, (2) only provides the information it collects and uses to the first-party online service, (3) has no independent right to the information it collects (except as necessary to provide the services it is paid for), and (4) has a contract with the first-party online service that outlines these restrictions. A third-party online service is a service operated by a for-profit or nonprofit organization that is not considered a first-party online service under the measure.

Places Restrictions on Computing Services. The measure places various restrictions on online and cloud computing service providers regarding the use of personal information of California residents. The measure defines personal information to include (1) various forms of identification (such as a driver's license number), (2) contact information (such as an e-mail address), (3) financial information (such as a credit card number), (4) information that could be used to identify a particular individual or device (such as an IP address), and (5) an individual's online activity. Specifically, the measure:

- ***Restricts First-Party Online Services From Sharing Personal Information.*** The measure restricts a first-party online service from requiring that an individual provide consent to the tracking of his or her personal information as a condition of accessing certain content or services. In addition, if an individual sends the first-party online service a DNT signal, the service cannot share, sell, or transfer personal information of that individual to another entity. The measure defines a DNT signal as any means of communication used by individuals to request that their personal information not be tracked. Based on the way the measure is written, it is unclear if government entities would be considered first-party online services. Courts could potentially interpret this measure to apply to government entities providing first-party online services, and such entities could be prohibited from information sharing.
- ***Requires Third-Party Services to Comply With DNT Signals.*** The measure specifies that an operator of a third-party online service shall not track the personal information of an individual who sends a DNT signal, except as necessary to prevent fraud or to comply with a request of a law enforcement agency.
- ***Restricts Use of Personal Information by Certain Cloud Computing Services.*** Under this measure, cloud computing services that provide service to state or local governmental institutions, as well as public or private educational institutions, cannot

use any personal information collected for any purpose other than directly providing services to those institutions. The measure defines a cloud computing service as any service that connects computers using real-time communications.

Changes Related to Litigation and Civil Penalties. The measure creates a legal presumption that the tracking of personal information in a manner prohibited by the measure caused harm to the individual whose information was tracked. This is a change from current law, which typically requires that individuals prove that they were harmed by the tracking of their personal information. The measure allows such individuals, the California Attorney General, any district or city attorney, or county counsel to bring civil action against operators of any online service that violates the restrictions established by this measure. Such online operators would be subject to a civil penalty not to exceed $10,000 per violation, with the penalty revenue going to the jurisdiction on whose behalf the action was brought. If the action is brought by an individual, the penalty revenue would go to the state.

In addition, the measure states that when the action is brought on behalf of individuals, the online operator would be required to surrender all consideration received in connection with the violation. For each violation, the measure requires the operator to pay individuals the greater of $1,000 or actual damages. However, in cases where the operator tracked the individual in knowing and willful violation of the measure, the measure requires the operator to pay the individual the greater of $10,000 or actual damages for each violation.

Fiscal Effects

The magnitude of the fiscal impact of the measure would depend on how the courts interpret various provisions of the measure (such as whether government entities would be considered first-party online services), as well as how governments, private entities, and the public respond to the new law. As we discuss below, the measure would (1) increase costs related to state courts and the enforcement of the measure and (2) create revenue from new civil penalties it authorizes. For the purposes of our analysis, we assume that government entities are not considered first-party online services.

Additional Costs Related to State Courts and Enforcement. To the extent this measure leads to more or lengthier civil actions against online service operators, there would be additional workload for state courts. In addition, the California Attorney General's office and local governments would experience increased costs to the extent they brought civil action against online service operators accused of violating provisions of the measure. The magnitude of these workload costs is uncertain and would depend on how individuals, state and local governments, and private entities respond to the law. Depending on these factors, the above costs could reach millions of dollars in some years.

Civil Penalty Revenue. The measure would result in increased penalty revenue for state and local governments resulting from the new civil penalties authorized by the measure. The actual amount of revenue is subject to significant uncertainty and would depend on how the courts interpret various provisions of the measure, as well as how governments, private entities, and the public respond to the new law. Depending on these factors, the increased revenue could reach the tens of millions of dollars in some years.

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

- Increased costs potentially reaching millions of dollars in some years to state and local governments primarily from additional or more costly civil actions and increased court workload.
- Increased penalty revenue potentially reaching tens of millions of dollars in some years to state and local governments resulting from new civil penalties authorized by the measure.

Sincerely,

_____

Mac Taylor
Legislative Analyst

_____

Michael Cohen
Director of Finance