

September 9, 2013

Hon. Kamala D. Harris  
Attorney General  
1300 I Street, 17<sup>th</sup> 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 constitutional initiative (A.G. File No. 13-0008 Amendment #1-S) relating to personal privacy.

## Background

***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.

***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

***Expands Definition of What Is Considered Confidential Personal Information.*** This measure expands the type of personal information that would be considered confidential. Specifically, the measure states that confidential personal information is information provided by a person to a public agency, private entity, or individual to be used for a governmental or commercial purpose and that can be linked to that person. However, information contained in public government records would not be considered confidential. Under the measure, state and local governments and private entities would be required to use all reasonable means to protect

confidential personal information in their possession and be prohibited from sharing such information without the individual's permission. Entities could disclose personal information without permission if it would serve a compelling interest and there is no reasonable alternative to accomplishing that interest.

***Changes Presumption of Harm for Privacy Lawsuits.*** The measure creates a legal presumption that the unauthorized disclosure of confidential personal information caused harm to the individuals whose information was disclosed. This is a change from current law, which requires individuals bringing lawsuits to prove that they were harmed by the unauthorized disclosure.

### **Fiscal Effects**

This measure would result in unknown but potentially significant costs to state and local governments. The actual magnitude of these costs would depend on how the courts interpret various provisions of the measure, the extent to which subsequent legislation clarifies certain provisions, as well as how governments, private entities, and the public respond to the new law. As we discuss below, increased costs could result from (1) additional or more expensive lawsuits filed against government agencies, (2) increased workload for state courts, (3) the implementation of increased data security measures, and (4) changes to government information-sharing practices.

***More Frequent or Costly Lawsuits Against Governments.*** Changing the presumption of harm in privacy cases would make it easier for individuals to win privacy lawsuits against state and local governments. As a result, more people may file lawsuits in state courts and those lawsuits could take more time to resolve, likely resulting in additional government costs for litigation. Governments could also face additional costs for payments to plaintiffs if courts more often find that government agencies did not properly protect personal information or otherwise disclosed such information without authorization. The magnitude of these potential costs is unknown and would depend on how the courts, governments, and individuals respond to the new law. For example, government agencies may respond by changing their data security and information-sharing practices in order to avoid lawsuits, leading to little or no increase in the number of these lawsuits that are filed. On the other hand, even if the measure leads to a reduction in the number of unauthorized disclosures, each disclosure may be more likely to lead to a lawsuit, causing an increase in lawsuits.

***Additional Costs to State Courts.*** To the extent this measure leads to more or lengthier privacy lawsuits against governments or private entities, there would be additional workload for state courts. The magnitude of these workload costs is uncertain and would depend on how individuals, governments, and private entities respond to the law.

***Costs to Improve Data Security.*** State and local governments might choose to invest in additional technologies, new procedures, or additional staff training in order to avoid or comply with lawsuits. The magnitude of these costs is unknown but could be significant. In part, how governments respond to the new law could be affected by how the courts interpret certain provisions of the measure, such as what constitutes reasonable efforts by governments to protect personal information from unauthorized disclosure.

***Changes to Government Information-Sharing Practices.*** This measure could affect what government information-sharing practices are permissible under current law. For example, state and local agencies currently share personal information to carry out government functions such as law enforcement, education, and research. Under the measure, government agencies could be more limited in their ability to share personal information without first obtaining each person's permission. This could result in state and local government agencies incurring additional costs to obtain such permission, as well as to change certain operations where obtaining permission is not feasible.

### **Summary of Fiscal Effect**

This measure would have the following fiscal effect:

- Unknown but potentially significant costs to state and local governments from additional or more costly lawsuits, increased court workload, data security improvements, and changes to information-sharing practices.

Sincerely,

---

Mac Taylor  
Legislative Analyst

---

Ana J. Matosantos  
Director of Finance