05/02/13

Honorable Assembly Member Lowenthal
California State Assembly
State Capitol Room
Sacramento, CA 95814

RE: AB 1291 Opposition

Dear Assembly Member Lowenthal:

The trade associations listed below have concerns with your proposed Assembly Bill 1291. As drafted, AB 1291 is overly broad, and would impose costly and unworkable mandates on California businesses, with little upside for consumers. While we have several concerns with AB 1291, our primary concerns include the overly-expansive and unworkable definition of personal information, the requirement that businesses provide names and addresses to whom the information has been "disclosed," and the somewhat counter-intuitive requirement that a California business reasonably verify a consumer's identity before turning over any requested information – a requirement that would likely require companies to collect sensitive personally identifying information, when they previously had none.

1. **Unworkable Definition of Personal Information.** As drafted, AB 1291 would expand categories of personal information to include "internet or mobile activity information" including, but not limited to, IP addresses. This broad expansion of personal information would essentially cover the most basic operational functions that enable the internet to work properly. For example, this expansion could encompass scenarios such as a consumer clicking to go to a new web page (an IP address is forwarded and shared with a "third-party") or a consumer choosing to download a new app, and the app developer needing to collect information to ensure that the app displays correctly on the consumer's specific device. The app developer might then need to share that information with its partners to ensure that any content is displaying correctly.

Under AB 1291, website operators and app developers would be required to log millions of these types of back-end operational transactions every month in order to provide consumers with access. Companies would quickly become overwhelmed by the sheer scale of the data retention and retrieval mandates. Consumer privacy would be undermined as companies were forced to retain more data, for longer periods of time. Furthermore, this type of operational data would be of little use to consumers, who would be swamped by the sheer volume of technical server logs, meant only to be understood by computers communicating with other computers.

While AB 1291 does appear to recognize the importance of allowing businesses to not have to "disclose" information as it is "reasonably necessary" to address security or technical issues, this provision is ambiguous, and would leave many businesses big and small, collectively scratching their heads as to

whether or not they were using "internet or mobile activity information" (which is now personal information) to perform "reasonably necessary" security or technical functions.

2. **Disclosure of Information Shared With Third-Parties.** AB 1291 calls for California businesses to provide to consumers access to, or copies of, all of the various categories of personal information identified that were shared with third parties (or retained by the website operator) in the preceding 12 months, within 30 days of the consumer's request. In addition to the above, website operators would also have to provide the name and address of every third-party to whom any of this "personal information" was provided to – the sheer scope of what AB 1291 is calling for here would place enormous financial and regulatory burdens on California businesses, both big and small. While AB 1291 does proffer that businesses need only provide this information as "reasonably available" to business, it is incredibly difficult for California businesses to know what "reasonably available" means, given the breadth of categories of information now being deemed personal information.

And that's just the start. Beyond the troubling characterization of IP addresses as "personal information," AB 1291 also includes the following categories of "personal information" – content (including text and photographs) generated by a consumer, commercial information, including records of property, educational information, etc. Going by these incredibly broad categories of personal information, social networking sites like Facebook might not be allowed to work with advertisers to sell inventory without creating a massive access database, as Facebook might be deemed to be "sharing" "personal information" with a "third-party." By some recent industry estimates, Facebook serves almost 7 billion ad impressions daily. Multiply that number by 12 months and the mandates created by AB 1291 become completely unworkable.

3. **Verifying A Consumer's Identity Before Disclosure.** While at first glance it would appear that the provision allowing a business to not disclose any information to a consumer without first verifying the consumer's identify is a safeguard for both consumers and businesses, this provision actually highlights one of the counter-intuitive results of AB 1291's approach towards protecting consumer's information privacy. By classifying such incredibly broad categories of information as "personal information", AB 1291 sets up a scenario where a business would potentially need to request sensitive personal information such as name, address, email address, social security number, etc., for purposes of disclosing to a consumer that "personal information" such as an IP address or device identifiers were shared. The exchange of sensitive personally identifiable information for a log of IP addresses is clearly not the goal of AB 1291, but would be the anti-privacy protection result.

It would appear the goal of AB 1291 is to give California consumers a clear and easy way to find out what kind of information is being collected online, and to give consumers options. This is a goal shared by the online advertising industry. In 2009, the trade associations listed here were some of the key groups that formed the Digital Advertising Alliance (DAA) to run and administer the Self-Regulatory Principles for Online Behavioral Advertising, a Program designed to give consumers transparency and choice about how data is being collected and used online.

The DAA's Self-Regulatory Program for Online Behavioral Advertising gives consumers the ability to ascertain in real-time what types of third-parties are operating on websites being visited, and gives consumers the ability to opt-out of third party data collection and use. Since the program's launch in 2010, more than 23.5 million consumers have visited the DAA sites to learn about their advertising data choices, and last year alone, more than a million consumers have taken action via DAA to exercise their choice about how advertisers will use their data.

When a consumer exercises choice – whether against all third-parties or a few – the affected participants stop collecting and using web viewing data from the user's browser for interest-based advertising. In many ways, the DAA Self-Regulatory Program has already succeeded in setting a very high bar for giving consumers access and choice about how information is being collected and used online – consumers can simply choose to opt-out of having information collected by third parties, eliminating the need for complicated data registries and disclosure protocols.

We ask that you consider the above concerns before moving forward with AB 1291.

Respectfully,

American Advertising Federation
Association of National Advertisers
Interactive Advertising Bureau

cc: Members, Assembly Committee on Judiciary
Drew Liebert, Consultant, Assembly Committee of Judiciary
Mark Redmond, Consultant, Assembly Republican Caucus Office of Policy