# California Expands Online Privacy Protections, Requiring "Do Not Track" Disclosures and Imposing New Breach Notification Requirements

October 4, 2013

On September 27, California Governor Jerry Brown signed into law two bills that expand online privacy protections for California consumers. Both will take effect January 1, 2014. The first, AB 370, amends the California Online Privacy Protection Act (Cal. Bus. & Prof. Code § 22575 *et seq.*) – the California law that requires the conspicuous posting of a privacy policy on all commercial websites that collect the personally identifiable information ("PII") of California residents. The existing law identifies the content that each privacy policy must contain, which includes the categories of PII that the website collects and that the website may share with third parties. Website operators who fail to provide these disclosures will be given a warning and 30 days to comply with the law.

The amendments will require that each privacy policy also disclose how the website operator responds to mechanisms, such as "Do Not Track" signals, that provide consumers with the ability to exercise choice regarding PII collection over time and across third-party websites. Website operators may satisfy this requirement by providing a clear and conspicuous hyperlink in the privacy policy that links to a description, including the effects, of any program or protocol the operator follows that offers consumers that choice.

The second bill, SB 46, amends California's data breach notification law (Cal Civ. Code § 1798 *et seq.*), adding to the definition of "personal information" certain information that would permit access to an online account, and imposing additional disclosure requirements if a breach involves personal information that would permit access to an online account or email account. Specifically, the legislation adds to the definition of personal information "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." A breach of this information, if unencrypted, of any California resident would trigger the state's data breach notification obligations.

In the case of disclosure of this type of personal information, however, a company will be permitted to notify affected California residents by alternative means. If the breach involves no other personal information, a company may notify the affected resident in electronic or other form that directs the resident to change his/her password and security question or answer, as applicable, or to take other steps appropriate to protect the affected online account and all other online accounts with the same user name or email address and password or security question and answer.

However, if the breach involves the login credentials of an email account furnished by the company, it cannot provide notification to that email address, but may provide notice by: (1) one of the

methods currently permitted under the law for notification of a breach of unencrypted personal information (written notice, electronic notice, or, if certain conditions are met, substitute notice); or (2) by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the company knows the resident customarily accesses the account.