Published on *The National Law Review* https://natlawreview.com

California Enacts New Data Privacy Laws

Article By:

James M. Chadwick

Rachel Tarko Hudson

As part of a flurry of new privacy legislation, California Governor Jerry Brown signed two new data privacy bills into law on September 27, 2013: S.B. 46 amending California's data security breach notification law and A.B. 370 regarding disclosure of "do not track" and other tracking practices in online privacy policies. Both laws will come into effect on January 1, 2014.

New Triggers for Data Security Breach Notification

California law already imposes a requirement to provide notice to affected customers of unauthorized access to, or disclosure of, personal information in certain circumstances. S.B. 46 adds to the current data security breach notification requirements a new category of data triggering these notification requirements: A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Where the information subject to a breach only falls under this new category of information, companies may provide a security breach notification in electronic or other form that directs affected customers to promptly change their passwords and security questions or answers, as applicable, or to take other steps appropriate to protect the affected online account and all other online accounts for which the customer uses the same user name or email address and password or security question or answer. In the case of login credentials for an email account provided by the company, the company must not send the security breach notification to the implicated email address, but needs to provide notice by one of the other methods currently provided for by California law, or by clear and conspicuous notice delivered to the affected user online when the user is connected to the online account from an IP address or online location from which the company knows the user ordinarily accesses the account.

Previously, breach notification in California was triggered only by the unauthorized acquisition of an individual's first name or initial and last name in combination with one or more of the following data elements, when either the name or the data elements are unencrypted: social security number; driver's license or state identification number; account, credit card or debit card number in combination with any required security or access codes; medical information; or health information. S.B. 46 not only expands the categories of information the disclosure of which may trigger the

requirement for notification, it also—perhaps unintentionally—requires notification of unauthorized access to user credential information even if that information is encrypted. Thus, S.B. 46 significantly expands the circumstances in which notification may be required.

New Requirements for Disclosure of Tracking Practices

A.B. 370 amends the California Online Privacy Protection Act (CalOPPA) to require companies that collect personally identifiable information online to include information about how they respond to "do not track" signals, as well as other information about their collection and use of personally identifiable information. The newly required information includes:

- How the company responds to "do not track" signals or other mechanisms that provide consumers the ability to exercise choice over the collection of personally identifiable information about their online activities over time and across third-party websites or online services, if the company collects such information; and

- Whether third parties may collect personally identifiable information about a consumer's online activities over time and across different websites when a consumer uses the company's website.

These disclosures have to be included in a company's privacy policy. In order to comply with the first requirement, companies may provide a clear and conspicuous hyperlink in their privacy policy to an online description of any program or protocol the company follows that offers the user that choice, including its effects.

It's important to note that the application of CalOPPA is broad. It applies to any "operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service." As it is difficult to do business online without attracting users in technologically sophisticated and demographically diverse California, these provisions will apply to most successful online businesses.

What to Do

In response to the passage of these new laws, companies should take the opportunity to examine their data privacy and security policies and practices to determine whether any updates are needed. Companies should review and, if necessary, revise their data security breach plans to account for the newly added triggering information as well as the new notification that may be used if that information is accessed. Companies who collect personally identifiable information online or through mobile applications should review their online tracking activities and their privacy policies to determine whether and what revisions are necessary. The California Attorney General interprets CalOPPA to apply to mobile applications that collect personally identifiable information, so companies that provide such mobile apps should remember to include those apps in their review and any update.

National Law Review, Volume III, Number 292