NOVEMBER 18, 2013

LTN
LAW TECHNOLOGY NEWS

An ALM Publication

California Tightens Privacy Protection

Part 1 of 2: New California data privacy laws impose restrictions on third-party tracking and data breach notification

Alexander Southwell

California has a reputation of developing innovative regulation to address new technology—such as designing and implementing a range of laws intended to safeguard the privacy of consumer data against phishing, malware and cyberbullying. Recently, the California legislature passed three laws that significantly alter the privacy landscape and impose a new set of responsibilities that arguably apply to any company doing business in the state.

This article, part one of two, explains the California Privacy Policy Law and amendments to California's Data Breach Notification Law, and suggests how companies might comply with the new requirements set forth in each. Part two addresses the "Delete Button" law, which codifies minors' ability to request deletion of certain information posted online.

Privacy Policy Law

Assembly Bill 370, California's Privacy Policy Law, amends the California Online Privacy Protection Act to require additional disclosure in corporate privacy policies. Intended to facilitate transparency as to how a company tracks and shares user data, it requires disclosures dealing with three areas: 1) "do not track" signals; 2) third-party tracking; and 3) conspicuous opt-out notices.

"Do not track" signals: A.B. 370 requires companies to disclose how they respond to "do not track" signals. A "do not track" signal is an HTTP header field emitted by an Internet browser that instructs websites to cease all tracking activity. The Federal Trade Commission has informally called for companies to honor "do not track" requests in its educational publications, though it has not introduced formal rules on the subject. Without a specific requirement to honor such signals, many companies choose to ignore them.

There are two notable features of this provision. First, the disclosure is not limited to "do not track" signals, but also includes "other [similar] mechanisms." Companies should be careful to ensure that they are equipped to deal with other "opt-out" mechanisms as they become available. Second, by its terms this provision applies to all tracking activity, regardless of the motivation behind the tracking. As a result, a company must report tracking conducted for internal research and development in addition to tracking for other purposes such as marketing.

Third-Party Tracking

A.B. 370 requires companies to disclose whether third parties may collect personally identifiable information about a consumer's online activities. Previously, CalOPPA required companies to disclose only the "category" of third-parties with whom they share information that they themselves collected. Importantly, the amendment only requires companies to disclose whether third-parties collect information; not details regarding what information

the third-parties track. Nonetheless, companies should ensure they fully understand whether and how third-parties track user activity on their web sites, and update their privacy policies accordingly.

Opt-Out Disclosures

A.B. 370 also permits a company to satisfy the "do not track" disclosure requirement by providing a "clear and conspicuous" hyperlink in its privacy policy to an explanation of the company's opt-out program, and a mechanism for the user to opt-out of the company's tracking practices. However, linking to opt-out procedures only satisfies a company's obligation to disclose how it treats "do not track" signals, and does not satisfy A.B. 370's third-party tracking disclosure requirement.

Ensuring Compliance

The law does not provide clear guidance as to its geographic scope. By its terms, it applies to any company that owns or operates a website and collects California residents' personally identifiable information through the Internet. This would presumably include all companies that collect PII , so long as the company's website has had a single visitor residing in California. In view of this provision's extraordinary scope, along with California's increased focus on privacy policies, companies nationwide should assess whether they comply with this law.

Data Breach Notification Law

Senate Bill 46 broadens the scope of California's data breach notification statute. It enacts California Civil Code §§ 1798.29 (relating to government agencies), and 1798.82 (relating to persons and businesses), which require companies and government agencies to notify California residents when they experience a breach of user names or email addresses that would allow access to the user's account.

California already requires businesses to notify consumers about the unauthorized acquisition of their PII. Its data breach notification statute, passed in 2002, served as model for a number of states that followed suit with nearly identical statutes.

S.B. 46 expands the definition of "personal information" in the statute to encompass credentials that would allow an unauthorized person to log into someone's online accounts. S.B. 46 requires businesses to notify consumers of any breach involving "a user name or email address, in combination with a password or security question and answer that would permit access to an online account."

The amendment also governs how a company must notify consumers about the unauthorized acquisition of their login credentials:

For breaches of login credentials that would not allow access to an email account, companies may provide consumers notice of the security breach via email or any other permissible method.

For security breaches that do involve email login credentials, businesses cannot satisfy S.B. 46's notice requirement via email notice. Instead, businesses must provide notice through one of several permissible methods:

- "Clear and conspicuous notice" to the user when he or she is connected to their online account from an IP address or online location from which the business knows the user customarily accesses their account.
- Written notice, which is often quite costly.
- Electronic (but non-email) notice in compliance with federal law.

The amendments take effect January 1, 2014. To ensure compliance, companies should investigate whether they keep track of user IP addresses or log-in locations. Companies that do not currently record this information should consider doing so, to avoid having to issue costly written notice in the event of a data breach.

New York-based Alexander Southwell is a partner and co-chair of the information technology and data privacy practice at Gibson Dunn & Crutcher. Email: Asouthwell@gibsondunn.com. California-based associates Joshua Jessen, Vivek Narayanadas, and Danielle Serbin, contributed to the article.