Foster Garvey

New California Requirements for Privacy Policies

Legal Alert
October 15, 2013

Garvey Schubert Barer Legal Update, October 15, 2013.

On September 27, 2013, California Governor Jerry Brown signed into law three new laws relating to the collection and protection of personally identifiable information (PII) of California consumers. These laws impose new requirements on operators of commercial websites or online services that collect personally identifiable information of California consumers, regardless of where the operator is located. As a result, clients collecting PII of California consumers will need to review and may need to modify their privacy policies.

Collection: Assembly Bill No. 370, amends the California Online Privacy Protection Act (CalOPPA) which requires operators of commercial websites or online services that collect PII, including first and last names, email addresses, social security numbers, and other data, about California consumers to conspicuously post their privacy policies. These policies must provide an effective date and descriptions of the types of data collected and disclosed, how a consumer can access and/or request changes to his or her PII, and how the operator will notify consumers of policy changes. AB 370 amends CalOPPA to require covered operators to update their privacy policies to include new disclosures. Specifically, the amended Act now requires that operators disclose:

How they respond to "Web browser do not track signals" or other mechanisms that allow consumers to choose whether and how PII about their online activities is collected over time and across third-party websites or online services; and

Whether other parties may collect such PII over time and across different websites when the consumer uses the operator's website or service.

Related Services

Commercial & IP Transactions

Government Contracts

Website and online service operators may satisfy the former requirement by providing a clear and conspicuous hyperlink in their privacy policy to an online location that describes any program or protocol the operator follows to offer consumer's choice as to how/whether PII is collected.

Protection: Governor Brown also signed into law Senate Bill No. 46 and Assembly Bill No. 1149, which amend California's data security breach notification laws to expand the list of data elements that qualify as "personal information," the release of which may trigger notification requirements. Generally, California law requires a business or state agency to notify California residents whose unencrypted personal information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person. If that business or agency must notify more than 500 California residents of a single breach, then it also must submit a copy of the breach notification, excluding users' personal information, to California's Attorney General. The new laws require businesses and agencies to notify their users if there is a breach involving user names or email addresses which "in combination with a password or security question and answer" permit access to an online account. In the event of such a breach, users must be informed of it electronically or otherwise—but not via a compromised email address—and directed to change their passwords and/or security questions or answers, or to take other necessary steps to protect their online account.

Takeaway: Any client operating a website or providing an online service that collects personal information from California residents should review its existing privacy and breach notification policies and update them as needed to comply with the new California requirements. Clients should keep in mind that this is an area that is in flux and that rules regarding privacy, data collection, data security and breach notification abound at both the state and federal level and are subject to change. For example, new rules have recently gone into effect for clients that collect or have access to PHI, children's information, and government data. And, by now most states have enacted data breach rules. These new laws also underscore the benefits of encrypting data to escape some of the onerous breach notification requirements.

For guidance on these matters contact:

Scott G. Warner: sgwarner@gsblaw.com (Data Protection, Technology and IP)
Benjamin Lambiotte: blambiotte@gsblaw.com (Government Contracts)
Stephen Rose: srose@gsblaw.com (Healthcare).