Privacy & Security

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy & Security Alert

JUNE 5, 2014

Making Privacy Practices Public: the California Attorney General's New Guidelines Keep the Focus on the Consumer's Perspective and New Disclosure Requirements

BY CYNTHIA LAROSE, CIPP AND JAKE ROMERO, CIPP

In 2013, the California Online Privacy Protection Act (CalOPPA) was amended to require web sites and other online services to make additional privacy policy disclosures related to online tracking transparency. Within the online privacy policy that is required under CalOPPA, web site and online service operators are required to disclose (1) how the operator responds to browser Do Not Track (DNT) signals and similar requests and (2) whether any third parties are permitted to track users of the service. By the time the amendment to CalOPPA went into effect on January 1, 2014, however, it was clear that there would be considerable confusion about how to comply with the new requirements. Although it is understood in general terms, there is no universal standard for responses to DNT and industry efforts to define precisely what it means to honor a DNT response had stalled.

As part of a broader attempt to provide guidance regarding compliance with CalOPPA, the California Attorney General's Office has released a set of guidelines titled Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy. Although the guidelines are not law (and in some cases make recommendations beyond what is minimally required by CalOPPA), implementing the recommended practices can help online service providers avoid regulatory consequences such as Attorney General enforcement actions or even Federal Trade Commission enforcement actions. In addition to providing an overview of the well-established CalOPPA notice content requirements, the guidelines include a number of best practices covering fundamental aspects of how notice is provided:

Do Not Track Disclosures. Although considerable space is devoted to addressing the new DNT disclosure requirements, the guidelines are unlikely to satisfy those seeking additional clarity regarding how to formulate a description of a web site's DNT response. Since there is no universal standard for DNT, any online service provider that makes an unqualified promise to honor DNT takes on a substantial risk of breaking that promise. Instead, the guidelines recommend that service operators provide consumers with a description of the tracking programs being used in connection with the service, in easy-to-locate sections with a clearly identifiable heading. DNT disclosures should describe all tracking of users that is done over time and across third party web sites, either directly by the service provider or by a third party. If tracking programs are in place, the policy should disclose how, or if, users whose browsers send a DNT signal are treated differently from other users. Where tracking is conducted by third parties, the guidelines recommend that the service provider consider whether the third parties it authorizes to track users will follow the service provider's DNT policy. If an online service provider cannot ensure that its third-party trackers comply with its DNT policy, then the consumer should be informed. Although CalOPPA permits linking to an online tracking consumer choice program as an alternative to making certain disclosures, the guidelines make it clear that the online service provider must follow the program that it links to, and still retains the risk that an outside link is not sufficiently clear to permit users to control tracking online.

Scope and Availability. Issues of scope and availability need to be reconsidered as the ways in which consumers receive products and services becomes more complicated. Any business that collects information about its customers offline should clarify whether its online privacy policy applies to those offline collection activities. Mobile application providers should ensure that the privacy policy is available both (1) prior to download and (2) after download, within the application itself.

Readability. The guidelines recommend plain, straightforward language that avoids legal or technical jargon. In particular, consideration should be given to the format and readability of mobile application privacy policies, since the user will be accessing those policies on a smaller screen. Simply moving your clunky online privacy policy to the small screen is not recommended.

Collection and Sharing of Data; Security. Requiring descriptions of the categories of personal information collected and any third parties with whom information is shared is not new. The guidelines reiterate the minimum requirements for describing collection, use and sharing, and also recommend certain best practices that are not strictly required under the statute, such as providing links to the privacy policies of third parties with whom information is shared and specifying retention periods for each type of personally identifiable information collected. The guidelines also recommend including a general description of security measures used to protect consumer information.

Individual Choice and Access; Accountability. As we recently discussed in connection with the Federal Trade Commission settlements with Credit Karma and Fandango, issues related to consumer control of information, including access to provide feedback and request information, are key considerations in enforcement actions. Online service providers should provide easy-to-follow instructions for updating or deleting account information, and give consumers a direct point of contact to request changes to the handling of personal information to ensure responsiveness. Rather than relying on a general customer service number, online service providers should consider using a designated line that specifically addresses security concerns and feedback as well as information requests from consumers.

Effective Date. In addition to providing the effective date on the top of each privacy policy, online service providers should proactively define a process for implementing privacy policy updates (including the mechanics of providing notice to affected users and assessing whether affirmative consent from consumers will be needed to make changes) and describe that process in the policy. As we recently discussed, making changes to privacy policies can create a number of issues with regulators as well as consumers.

Although they do not address some of the recent issues created by the new regulations, the guidelines are an excellent resource for seeing the thought process and focus that the Attorney General's office brings to enforcement actions. In particular, the guidelines continually emphasize the consumer perspective and ensuring readability and access. There is no time like the present to take a step back and review your policies and practices with a fresh set of eyes and from the outlook of your product's users.

* * *

View Mintz Levin's Privacy & Security attorneys.

Read and subscribe to *Privacy & Security Matters* blog.