Client Alert

pillsbury

Antitrust & Competition | Social Media & Games
Consumer & Retail | Litigation
Privacy, Data Security & Information Use | Communications

June 5, 2014

California AG Issues New Privacy Policy and "Do Not Track" Compliance Guidelines, Announces Proactive Enforcement

by Andrew D. Lanphere, Catherine D. Meyer, Roxane A. Polidora and Jacob R. Sorensen

The California Attorney General recently released a series of guidelines to assist with compliance with the California Online Privacy Protection Act of 2003 (CalOPPA), which was amended to require new data collection and Do Not Track disclosures. These guidelines offer assistance regarding the form and content of operators' privacy policies. The AG has stated she will actively enforce operators' compliance with CalOPPA, including through litigation. Operators of websites and online services that are used or visited by California residents should ensure as soon as possible that their privacy policies comply with the AG's guidelines.

California Online Privacy Protection Act's New Requirements Regarding Data Collection and Do Not Track Disclosures.

CalOPPA, Cal. Bus. & Prof. Code §§ 22575-22579, has since 2003 required "operators"[1] of commercial websites and online services that collect "personally identifiable information"[2] of California residents to conspicuously post their privacy policies. An operator violates CalOPPA if its privacy policy fails to comply with the statute's disclosure requirements either (1) knowingly and willfully or (2) negligently and materially. Cal. Bus. & Prof. Code § 22576. The Attorney General has previously filed suit for CalOPPA violations

[1] "Operator" means any person or entity that owns a website or online service operated for commercial purposes that collects and maintains personally identifiable information from a California resident who uses or visits the website or online service. "Operator" does not mean third parties who operate, host or manage, but do not own, a website or online service. Cal. Bus. & Prof. Code § 22577(c).

[2] "Personally identifiable information" means "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form" and expressly includes (1) first and last names; (2) home or other physical addresses; (3) e-mail addresses; (4) telephone numbers; (5) social security numbers; (6) any other identifier allowing consumers to be contacted online or physically; and (7) information concerning a consumer that the operator maintains along with any of the foregoing six types of information. Cal. Bus. Prof. Code § 22577(a).

seeking injunctive relief and civil penalties under Bus. & Prof. Code § 17200, on the theory that the improper privacy policy constituted an unlawful business practice.

As of January 1, 2014, CalOPPA requires that privacy policies additionally describe (1) how the operator responds to "Do Not Track" browser signals ("DNT Signals") or "other mechanisms" that give a consumer the ability to indicate the consumer does not want his or her personally identifiable information collected and tracked; and (2) the possible presence of other parties conducting online tracking on the operator's website or online services. Cal. Bus. & Prof. Code § 22575(b)(5)-(6). In lieu of the first requirement to describe how the operator responds to DNT Signals, the operator can provide a "clear and conspicuous" link in the privacy policy to a "program or protocol" that offers consumers a choice about online tracking, along with a description of the program or protocol and the effects it has on participating consumers. Cal. Bus. & Prof. Code § 22575(b)(7).

The California Attorney General's CalOPPA Recommendations for Compliance

On May 21, 2014, the Privacy Enforcement and Protection Unit (the "Privacy Unit") of the California Attorney General's Office issued "Making Your Privacy Practices Public," which provides detailed, specific guidance regarding how operators of websites and online services should implement the requirements of CalOPPA as amended. These recommendations, which are summarized below, cover not only the disclosures required in operators' privacy policies, but also the style and format of the policies.

Guidance on New Disclosure Requirements

Do-Not-Track: The operator has two options for disclosing its responses to Do-Not-Track signals. First, preferably, it can include a section in the privacy policy labeled "How We Respond to Do Not Track Disclosures" that includes a description of how it responds to DNT signals. The AG suggested describing whether the operator treats browsers sending DNT signals differently than those that do not, whether it continues to collect personal information from consumers whose browsers send DNT signals and how it uses that information. Second, the operator may provide a link to a different website that offers a protocol giving consumers a choice about online tracking. The AG views the second alternative as less transparent for consumers. However, if this alternative is employed, the link should be conspicuous, and the landing page should disclose whether the program results in stopping the collection of a consumer's information across websites and online services over time and what the consumer must do to exercise the choice offered by the program. The privacy policy should give a brief description of what the third party program does and that it complies with CalOPPA.

Collection of personally identifiable information by third parties: The privacy policy must describe whether the operator permits third parties to conduct online tracking on the operator's website or online services and whether those third parties are or may be engaging in tracking consumers visiting the website or service. The operator should consider whether such activity is limited to approved parties, how the operator verifies that approved parties are not allowing unauthorized parties to collect information and how the third party's practices may differ from the operators' practices, if at all. Of course, the operator should confirm its actual practices before making disclosures.

Guidance on Pre-2014 CALOPPA Disclosure Requirements

Scope: The privacy policy should explain whether it applies only to online data collection, or to online and offline practices, and the entities (such as subsidiaries or affiliates) to which it applies.

Availability: The privacy policy should have a recognizable, descriptive title. It should be conspicuously available to users and potential users of the operator's website or online service using a link on the website's homepage and pages where data is collected or the application's platform page that is made conspicuous by its font, color or symbols.

Readability: The privacy policy language should be straightforward, plain English and non-technical or legalistic. The AG recommends short, active voice sentences, topic headings, and a format that provides easy reading, including on smaller screens.

Data collection: The privacy policy should disclose whether the operator collects personally identifiable information directly from the user or indirectly through third parties or cookies or similar technologies. The types of information collected should be reasonably specified by category. Collection of information from children under 13 should be disclosed in compliance with the Children's Online Privacy Protection Act.

Data use and sharing: The privacy policy must explain how the operator uses the personally identifiable information it collects and under what circumstances it shares that data with different categories of entities, such as affiliates, marketing partners and others.

Individual choice and access to personal information: The privacy policy should provide clear instructions on how consumers can exercise choices regarding the operator's collection, use, or sharing of personally identifiable information. The operator should honor those choices within a reasonable period of time. Operators should consider offering consumers the opportunity to review and correct their personal information under circumstances where the operator can verify the consumer's identity and access authority, particularly where sensitive information is involved. Changes to personal information should of course be documented through audit logs or transaction histories.

Security safeguards: The AG recommends that privacy policies describe the security measures used to safeguard personal information in the operator's care and the measures used to control information security practices of third parties with whom the operator shares consumers' personal information.

Effective dates and changes to the privacy policy: The operator should state the effective date of the privacy policy and explain how consumers will be notified of changes to the privacy policy. The AG suggests that operators not rely on changes to the privacy policy posted on the website or online services as the only means of notifying consumers of material changes.

Accountability: The privacy policy should identify a point of contact for consumers with questions or concerns about privacy policies and practices, at least including the contact's title and email or postal address and perhaps a toll-free telephone number staffed by trained personnel.

Enforcement

The Attorney General's Office has indicated that it will actively enforce operators' compliance with the Attorney General's CalOPPA recommendations. In an interview given to *The New York Times*, a member of the Privacy Unit stated that the Attorney General's Office "would review companies' privacy policies and work with them to make sure they followed the new law. Those who don't comply will receive 30-day warnings before facing potential litigation from the state."[3]

[3] Vindu Goel, *California Urges Websites to Disclose Online Tracking*, N.Y. Times, May 21, 2014.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Andrew D. Lanphere (bio)
San Francisco
+1.415.983.1321
andrew.lanphere@pillsburylaw.com

Catherine D. Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Roxane A. Polidora (bio)
San Francisco
+1.415.983.1976
roxane.polidora@pillsburylaw.com

Jacob R. Sorensen (bio)
San Francisco
+1.415.983.1893
jake.sorensen@pillsburylaw.com

Sarah G. Flanagan (bio)
San Francisco
+1.415.983.1190
sarah.flanagan@pillsburylaw.com

Elsa S. Broeker (bio)
Austin
+1.512.375.4935
elsa.broeker@pillsburylaw.com