WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON PARIS LONDON MILAN ROME FRANKFURT BRUSSELS

CLIENT MEMORANDUM

Websites and Mobile App Providers Must Amend Their Privacy Policies to Comply with New "Do Not Track" Disclosure Requirements by January 1, 2014

December 16, 2013

AUTHORS

Frank Buono | **Barbara Block** | **Brenna Sparks**

On January 1, 2014, a new California law will take effect requiring the addition of two new disclosures to the privacy policies already required of any company that collects and maintains the personally identifiable information ("PII")[1] of a consumer residing in California. The new law (AB 370)[2] amends the state's Online Privacy Protection Act ("CalOPPA") and applies to anyone owning an Internet website or an online service and to mobile application ("app") developers and other mobile app companies—located either in or outside California—that could be accessed or used by California consumers. Companies affected by the law should review and revise their privacy policies by the effective date in order to avoid potentially significant penalties.

[1] The term "personally identifiable information" as broadly defined by CalOPPA 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, including any of the following: (1) A first and last name; (2) A home or other physical address, including street name and name of a city or town; (3) An e-mail address; (4) A telephone number; (5) A social security number; (6) Any other identifier that permits the physical or online contacting of a specific individual; (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision."

[2] A copy of AB 370 is available here.

CalOPPA currently requires the owner of any website or online service (an "operator") operated for commercial purposes that collects PII about a California resident through the Internet to conspicuously post a privacy policy that meets certain content requirements including, among other things, identifying the types of PII collected and the categories of third parties with whom that information is shared. In 2012, the California Attorney General's office interpreted CalOPPA to apply to mobile app companies as well.[3] The new law requires that companies subject to CalOPPA add the following new disclosures to those privacy policies:

- First, AB 370 requires an operator that collects PII about an individual consumer's online activities over time and across third-party websites and online services to disclose in its privacy policy how the company responds to browser "do not track" signals or other mechanisms that provide consumers with a choice regarding the collection of such information. A company may satisfy this requirement by revising its privacy policy to include the new disclosures or by providing a clear and conspicuous hyperlink to a webpage that contains a description, including the effects, of any program or protocol the company follows that offers consumers a choice about tracking.

- Second, the new law requires affected companies to disclose to users whether third parties may collect PII about the user's online activities over time and across different websites when a consumer uses the operator's website or online service. However, an operator is not required to disclose the identity of such third parties.

California has not mandated that operators honor a user's use of "do not track" mechanisms that may be built into the user's web browser, only that the operators provide users with a disclosure about how the website or mobile app will respond to such mechanisms. In general, "do not track" mechanisms are typically small pieces of code, similar to cookies, that signal to websites or mobile apps that the user does not want his or her website or app activities tracked by the operator, including through analytics tools, advertising networks, and other types of data collection and tracking practices. Unfortunately, AB 370 does not define "do not track" or provide any guidance on how the broadly defined term "PII" will be interpreted and applied in this context.

A violation of the law can incur a civil fine of up to $2,500 per violation. Separately, the California Attorney General maintains that *each* non-compliant mobile app download constitutes a single violation and can trigger the fine.

Recommendations:

- Operators should review their websites, other online services, and mobile apps to determine (i) the tracking methods used and how the services respond to "do not track" settings; and (ii) whether third parties conduct tracking activities on their websites or other services. If an operator does not respond to "do not track" signals, it

[3] *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law*, Office of the Attorney General of California (Oct. 30, 2012), copy available here.

will likely be sufficient to indicate this fact in the privacy policy; if an operator responds to such signals, the privacy policy should disclose how the operator responds.

- Given the uncertainties surrounding the definition of "do not track," operators would be well advised to broadly interpret "do not track" mechanisms and to update their policies over time as their practices change. Additionally, as noted, there has been no further explication on how parts of CalOPPA's definition of PII will be interpreted in the "do not track" context, specifically the part of the definition that treats as PII "[a]ny other identifier that permits the physical or online contacting of a specific individual." Although not entirely clear, the intent of this amendment is likely to cover various types of tracking, including cookies that track a user's website or online activities using a unique identifier, even if the cookie does not collect or store any "traditional" PII such as user name or email address. To be safe and to avoid potentially significant fines and penalties, operators may wish to consider any tracking of users' website or app activity as falling within the scope of this amendment and therefore implement the above new disclosures by January 1, 2014.

If you have any questions regarding this memorandum or need assistance drafting the new disclosures for your website or mobile app privacy policy, please contact Frank Buono (202 303-1104, fbuono@willkie.com), Barbara Block (202 303-1178, bblock@willkie.com), Brenna Sparks (202 303-1145, bsparks@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Paris, London, Milan, Rome, Frankfurt and Brussels. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

December 16, 2013