Extracted from *Law360*

# Inside Calif.'s Proposed Guidance For Do-Not-Track Law

Law360, New York (December 19, 2013, 6:36 PM ET)

On Dec. 10, 2013, the Privacy Enforcement and Protection Unit of the California Office of the Attorney General held a meeting in San Francisco for interested stakeholders to discuss best practices in light of the assembly's enactment of A.B. 370, California's new do-not-track disclosure law that goes into effect on Jan. 1, 2014.

The new law provides that operators of websites, online services and mobile applications must amend their privacy policies as of the new year to either (1) disclose how they respond to do-not-track signals from Internet browsers or other consumer choice mechanisms regarding the collection of behavioral tracking data; or (2) link to an online location containing a description of a consumer choice program the operator follows and explain the effects of that program. The new law also requires these operators to disclose the type and nature of any third-party tracking occurring on their sites, services or apps.

The AG staff focused the discussion with stakeholders on what should constitute "best practices" regarding do-not-track disclosures, rather than on what would be required for businesses to simply comply with the new disclosure requirements created by passage of A.B. 370. With respect to A.B. 370, however, staff observed the law's disclosure requirements focus on "collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services" (Section 22575(b)(5) of the California Business and Professions Code).

The staff observed that this statutory language requiring disclosures about the collection of behavioral data makes no mention about the use of that behavioral data for any particular purpose. This point was made in response to stakeholder questions as to whether the law itself required disclosures on a use-by-use basis, which the AG declined to specifically opine on in this meeting.

**Proposed Best Practices Guidelines for Behavioral Tracking**

In terms of best practices guidance that the AG is developing with respect to behavioral tracking practices, the staff suggested that such disclosures should not be limited to tracking simply for online behavioral advertising purposes, but should extend to other purposes for which behavioral data is collected by a business's website, online service or mobile app (e.g., market research, website analytics, website operations, fraud detection and prevention, or security). Additionally, the AG staff made it clear they would expect best practices for such operators to include language explaining the effects of any opt-out options that consumers choose.

In other words, if a link to an opt-out program or other choice mechanism is provided to consumers, staff said their view is that companies should explain what the link does and

does not do (e.g., opt out of targeted advertising, but continue to track for fraud and Web analytics purposes). When discussing their expectations in this manner, staff admitted that the best practices they would recommend in their upcoming guidance would go beyond the new do-not-track disclosure requirements in the California Online Privacy Protection Act (CalOPPA) established by A.B. 370.

Staff noted that the AG will aim to release a best practices guideline for behavioral tracking disclosures that includes industry input sometime in January 2014. It may be a standalone document or it may be folded in a broader guidance document containing the AG's overall best practice suggestions for constructing clear and concise privacy disclosures.

It was made clear by staff, however, that A.B. 370 compliance should not be delayed while companies whose websites, online services or mobile apps operating in California await the guidance release from the AG. Rather, such companies will be expected to comply with the law as of its effective date, Jan. 1, 2014. Further, the AG staff stated that it does not view the 30-day enforcement grace period to be applicable to companies with existing CalOPPA-compliant privacy policies, as the 30-day delayed enforcement by the AG would only apply to companies where no privacy policy is currently present.

Stakeholders from industry also asked whether links to recognized behavioral advertising opt-out programs would comply with A.B. 370 under the safe harbor provision (Section 22575(b)(7)), but the AG staff declined to provide legal opinions about the scope of the law and what would constitute compliance with it. Instead, they maintained the focus of the discussion on the development of the best practices guidelines described above.

In response, stakeholders urged that the best practices guidelines contain language — similar to the California AG's existing guidelines for mobile privacy — that the guidance goes beyond the requirements of existing California law regarding do-not-track disclosures. For example, in the mobile privacy guidance issued by the CA AG in January 2013, titled "Privacy on the Go: Recommendations for the Mobile Ecosystem," the executive summary stated, "The recommendations, which in many places offer greater protection than afforded by existing law, are intended to encourage app developers and other players in the mobile sphere to consider privacy at the outset of the design process."

The request by several industry stakeholders during this meeting for similar qualifying language in the proposed do-not-track guidance was motivated by a collective concern that any best practices guidance released by the AG without such language could be misconstrued by litigants as the AG's interpretation of what disclosures were required in order to comply with A.B. 370. These concerns are reflective of the threat to industry already posed by the current vibrant class action environment over behavioral tracking practices in which 183 class actions are pending around the country.

**Conclusion**

As the first state in the country to adopt a do-not-track disclosure law, California has established, for now, a de facto disclosure standard for all businesses in the country operating websites, online services or mobile apps that may be used by residents of California. Naturally, in the globally connected environment of the Internet, that means many businesses that operate online or in the mobile environment must review and modify their privacy policies to include behavioral tracking disclosures, if applicable to their operations, in order to be in compliance with the new California law as of its effective date of Jan. 1, 2014.

Additionally, the California AG's meeting on Dec. 10, 2013, invited industry and other stakeholders to discuss its soon-to-be-released best practices guidance on behavioral tracking disclosures that will go beyond the requirements of the new law. This indicates that heightened transparency of behavioral tracking practices will likely be expected by the AG going forward.

Businesses engaged in behavioral tracking of consumers for a variety of beneficial purposes — not just for targeted online advertising, but also for Web analytics, market research, fraud detection and security — must therefore assess the potential risks of not disclosing such behavioral tracking. They should also consider their need for additional privacy policy disclosures and/or compliance practices to avoid potential AG enforcement actions or class action litigation in light of the increased activity in the plaintiffs' bar.

Finally, California's action in passing a new do-not-track disclosure law and its push to rapidly develop guidance in this area may influence other states to take action in 2014 in the form of new legislation or regulatory guidance. The Federal Trade Commission and interested members of Congress will likely also monitor developments in California on behavioral tracking disclosures as they consider new public policy proposals in 2014 that have the goal of increasing the transparency of these data collection practices.

—By Paul G. Martino and Dominique R. Shelton, Alston & Bird LLP

Paul Martino is a partner in Alston & Bird's Washington, D.C., office and co-leader of the firm's privacy and security practice. Dominique Shelton is a partner in the firm's Los Angeles office.