ALSTON & BIRD LLP

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

MAY 27, 2014

California Attorney General Kamala Harris Releases Long-Anticipated Guidance Regarding Privacy Policy Notices

AG's Report, "Making Your Privacy Practices Public," Contains Recommendations for All Businesses Collecting Information from California Residents

By Dominique R. Shelton and Paul G. Martino

On May 21, 2014, California Attorney General Kamala Harris released "Making Your Privacy Practices Public," her office's long-anticipated guidance on privacy policies for businesses collecting personal information related to California residents (the "Report"). As discussed in prior Alston & Bird client advisories and privacy blog postings, the California AG's office has been drafting its guidance document since December 2013 and had previously solicited input from stakeholders regarding its proposed recommendations. *See*, *Privacy & Data Security Advisory*: Special Assistant Attorney General Speaks on Privacy Issues at Alston & Bird's Los Angeles Office. Among its other recommendations, the new guidance was issued to advise companies operating inside and outside of California on how to address the amendments to California's Online Privacy Protection Act ("Cal-OPPA") that went into effect on January 1, 2014. As conceived, the Report is designed to apply to all businesses, regardless of the country or state in which they operate, based on the California AG's position that Cal-OPPA applies to all companies that collect personal information about California residents through their websites, online services or mobile apps, even if the business has no other connection to California.

Under California AB 370, a bill enacted in late 2013, Cal-OPPA was amended to include three new sections (Cal. Bus. & Prof. Code Sections 22575(b)(5)-(7)). Effective beginning in 2014, the new amendments require operators of websites, online services and mobile applications to include in their privacy policy disclosures: (a) how they respond to do-not-track (DNT) signals from Internet browsers or other consumer choice mechanisms regarding the collection of behavioral tracking data; (b) as an alternative to the first requirement, link to an online location containing a description of a consumer choice program the operator follows and explain the effects of that program; and (c) disclose the type and nature of any third-party tracking occurring on their sites, online services or mobile apps. *See* Alston & Bird's earlier client advisories for more details:

Privacy & Security/Legislative & Public Policy Advisory: On Eve of New Law Taking Effect, California Attorney General Announces Upcoming Best Practices Guidelines for Do-Not-Track Disclosures; and *Privacy & Security/Legislative & Public Policy Advisory:* California Adopts Do-Not-Track Disclosure Law, Reflecting a Significant New Development in a National Trend to Improve the Transparency of Online and Mobile Privacy Practices.

The Report makes it clear that the plaintiffs' bar should not attempt to use the California AG's recommendations as a sword against companies in more than 200 behavioral tracking/DNT putative class actions pending around the country. Instead, the Report expressly states that:

> "The recommendations here, which in some places **offer greater privacy protection than required by existing law**, are not regulations, mandates or legal opinions. Rather, they are part of an effort to encourage the development of privacy best practices." *Report* at 3 (emphasis added).

That said, the Report does provide insight into how the AG's office perceives "best practices" in privacy disclosures and, more importantly, how these best practices may ultimately alter the AG's interpretation and enforcement of the provisions of Cal-OPPA with respect to all businesses engaged in the online collection of personal information related to California residents.

It should be noted that the Report's issuance comes on the heels of three other significant public policy reports about online privacy concerns that have been released in the same month. On May 1, 2014, two reports were released by The White House on Big Data: (1) "Big Data: Seizing Opportunities, Preserving Values"; and (2) "Big Data and Privacy: A Technological Perspective." For a summary of these reports, *see* Alston & Bird's blog post "The White House Releases Report on Big Data." No sooner than companies had digested those 136 pages of policy statements and recommendations on Big Data practices, the U.S. Senate Permanent Subcommittee on Investigations released on May 15, 2014, a 43-page report, "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy," which was accompanied by the subcommittee's corresponding hearing.

In light of these developments, this advisory summarizes the key recommendations and observations of the California AG contained in the Report, and concludes with a final analysis on the impact and potential far-reaching effects the AG's consumer privacy guidance may have on other state and federal policy makers.

Report's Key Recommendations and Related Privacy Statements

The key recommendations in the Report related to improving the transparency of businesses' "Big Data," online behavioral tracking, and data security practices are as follows:

California AG Believes Cal-OPPA Is Not Limited to California Companies. In referencing Cal-OPPA specifically, the Report confirms the AG's view on the extra-territorial impact of the law as follows: "While the law only applies to companies that collect personally identifiable information of California residents, the state's economic importance and the borderless world of online commerce extend the impact of this law to other jurisdictions." *Id.* at 3.

Online Behavioral Tracking/Do-Not-Track Guidance. Some of the Report's most pertinent statements in this age of regulatory interest in "Big Data" concern online behavioral tracking and DNT disclosures. The salient points are as follows:

- Despite the enactment of AB 370 and its amendments to Cal-OPPA regarding DNT disclosures and third-party tracking described above, the Report clarifies that "[t]here is no legal requirement for how operators of web sites or online services must respond to a browser's DNT signal." *Id.* at 6. To that end, the Report acknowledges that "[a]s of the end of 2013, the W3C group had not agreed upon what an operator or an advertising network should do when they receive a DNT browser header." *Id.* at 7.[1]

- A company need only make disclosures regarding responses to DNT browser settings or link to an opt-out "if the operator engages in the collection of personally identifiable information about a consumer's online activities over time and across third-party web sites or online services." *Id.* at 7.

- The California AG recognizes that the "new provisions do not prohibit online tracking, nor do they depend on a standard for how an operator should respond to a DNT browser signal or to any mechanism that automatically communicates a consumer's choice not to be tracked." *Id.* at 7.

- The Report states that "[p]roviding a description of your site or service's online tracking practices, and of the possible presence of other parties that may be tracking consumers, can help to make this invisible practice more visible." *Id.* at 11. This statement seems to echo some of the statements contained in the two White House reports on Big Data, noted above, which expressed concern regarding the alleged lack of transparency in the collection and creation of Big Data.[2] Similar sentiments also were expressed in the recent report of the Senate Permanent Subcommittee on Investigations.[3]

Disclose the Presence of Other Parties that Collect Personally Identifiable Information on Your Site or Service. The AG recommends not only that third-party tracking be disclosed as required by Cal. Bus. Prof. Code Section 22575(b)(6) (which was newly added by AB 370), but also that companies go above and beyond the law to consider inclusion of disclosures that answer these questions: (a) whether there "[a]re only approved third parties on your site"; (b) "[h]ow would you verify that the authorized third parties are not bringing unauthorized parties to the site" and (c) "[c]an you ensure that authorized third-party trackers comply with your Do Not Track policy." *Id.* at 12.

Data Security and Control of Third-Party Information Security Practices. In addition to explaining the site's own data security practices, the AG encourages privacy policies for companies to "[g]ive a general description of the measures you use to control the information security practices of third parties with whom you share customer personal information for any purpose." *Id.* at 14.

---

1 Note, this language has not been updated from prior drafts of the AG's guidance to reflect the W3C's April 24, 2014, draft recommendation regarding DNT signals that was released after the departure of major stakeholders from the group. *See,* Tracking Preference Expression (DNT) .

2 *See, "*Big Data: Seizing Opportunities, Preserving Values" (at 41-44) and "Big Data and Privacy: A Technological Perspective" (at 43-45).

3 *See*, "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy" (at 7, where the report states that the "complexity of the online advertising ecosystem makes it impossible for an ordinary consumer to avoid advertising malware attacks, identify the source of the malware exposure, and determine whether the ad network or host web site could have prevented the attack.")

Key Statements on Privacy Issues Beyond Big Data, DNT and Data Security. Beyond Big Data, behavioral tracking and data security recommendations, some additional noteworthy statements of the California AG contained in the Report are as follows:

- **Companies Should Presume that the California AG Envisions Instances when a Device Identifier Could Constitute Personally Identifiable Information under the Law.** The California AG observed in the Report that Cal-OPPA's definition of the term personally identifiable information "can be understood to include information that is collected passively by the site or service such as a device identifier or geo-location data."[4]

- **California AG Reiterates Her Interpretation that Mobile Apps Are "Online Services" Within the Meaning of Cal-OPPA.** The California AG acknowledges that Cal-OPPA only applies to websites and "online services," and that it "does not define 'online service.'" However, the Report goes on to reiterate the previous statements made by the California AG about her interpretation of the scope of Cal-OPPA's application to mobile services by reminding businesses whose apps are used by California residents that "the Attorney General has stated that a mobile application is one type of online service." *Id.* at 5-6.

- **Scope of Privacy Policy, Including Applicability to Subsidiaries and Affiliates.** In addition to describing what data collection practices are covered by the policy (e.g., online or offline), the California AG encourages operators of websites, online services and mobile applications to "[c]learly indicate what entities the Privacy Policy covers, such as subsidiaries or affiliates." *Id.* at 9.

- **Conspicuous Website Notice and Prior Availability of Notice Before Download of a Mobile App.** The Report recommends that the link to privacy policies from a website's homepage be "conspicuous by using larger type than the surrounding text, contrasting color or symbols that call attention to it." *Id.* In the case of a mobile app, the Report recommends providing a "link to the policy on the application's platform page, so that users can review the policy *before* downloading the application." *Id.*

- **Readability of Notice; Use of Graphics or Icons.** The Report recommends that privacy policies use plain language (not legalese), and that businesses consider using a layered notice format and "[g]raphics or icons [that] can help users easily recognize privacy practices and settings." *Id.* at 10. This recommendation was previously made by the California AG in the 2013 report "Privacy on the Go" (at 11), as well as by the FTC in its own mobile privacy guidance. In response to these developments, Alston & Bird has created a suite of icons and short-form disclosures that are available for licensing by its clients. You can learn more about Alston & Bird's privacy disclosure and icon program by visiting our website and viewing the video here.

---

[4] California Business & Professions Code Section 22577(a) defines "personally identifiable information" to include names, address, email, telephone number, social security number, "[a]ny other identifier that permits the physical or online contacting of a specific individual," and "[i]nformation 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." The AG stated, "It should be noted that the last two types listed above can be understood to include…a device identifier." *Id. at 6.*

- **Data Collection (Generally).** The Report calls for companies to describe how they "collect personally identifiable information on users or visitors from other sources." *Id.* at 10. The Report also calls for companies to be "reasonably specific in describing the kind of personal information you collect." *Id.* at 10.

Conclusion

Despite the recent push among policy makers for short-form website notices or just-in-time notices for mobile apps, the Report makes clear the view of California Attorney General Kamala Harris that there is still an important role for more comprehensive privacy policy disclosures that explain to the public the full range of a business' data privacy and security practices. On this fundamental point, the Report observes:

> "Shorter, contextual privacy notices hold great promise, particularly in the limited space available in mobile devices and other embedded technologies. But there is still an important role for the comprehensive privacy policy statement that provides a fuller picture of an organization's practices regarding the collection, use, sharing, disclosure and protection of personally identifiable information. Having to provide a comprehensive policy statement promotes data governance and accountability, requiring an organization to consider its data practices and then to ensure that its policies are complied with internally. In addition, like other transparency measures, a privacy policy that must be made public can serve as a catalyst, stimulating changes in practice. Comprehensive privacy policies also inform policy makers and researchers, whose findings often reach the general public through the media. And, as discussed below, a comprehensive privacy policy may be required by law." *Id.* at 5.

Similar observations on privacy policies were made by California Assistant Attorney General Jeff Rabkin, who has oversight authority for the AG's Privacy Enforcement Unit, in a discussion held at Alston & Bird's Los Angeles, California, office on May 13, 2014. *See, Privacy & Data Security Advisory:* Special Assistant Attorney General Speaks on Privacy Issues at Alston & Bird's Los Angeles Office.

As Attorney General, Kamala Harris is the chief enforcer of California privacy laws, including Cal-OPPA, currently the only state law in the United States that requires operators of websites, online services and mobile apps to publicly post privacy policies when personally identifiable information is collected about state residents. The AG office also sponsored AB 370, which as noted above was the bill enacted by California in late 2013 that amended Cal-OPPA to require disclosure of certain online behavioral tracking practices. Therefore, companies that collect personal information from California residents should familiarize themselves with the Report to understand how the California AG's office views compliance with the state's privacy laws and its own best practice recommendations as they pertain to the amended Cal-OPPA.

Beyond business practices involving the collection of personal information about California residents, corporate executives and counsel should consider the potentially broader impact of the California AG's guidance as a harbinger of national trends in data privacy law. This would not be the first time that the state of California has taken the lead on privacy or data security policy that may have a nationwide impact.

More than a decade ago, California became the first state to enact a data security breach notification law, which has served as the blueprint for the breach notification laws that exist today in 47 states and four

federal jurisdictions, including the District of Columbia and Puerto Rico. Although it has not yet passed a federal data breach bill, Congress has also been influenced by California's groundbreaking breach notification law, which has provided the basic framework for bills introduced in the Senate and House since 2005. California's amendment to its breach law in 2013 to cover breaches of account user names and passwords has also prompted similar proposals in Congress. *See*, *Privacy & Security/Legislative & Public Policy Advisory:* California Expands Data Breach Notification Law to Include Breaches of User Names and Email Addresses for Online Accounts.

More recently, in late 2013, California enacted a new law establishing digital privacy rights for minors (AB 568) which, upon its effective date of January 1, 2015, will prohibit certain content targeted advertisements to minors in California and require operators of websites, online services and mobile applications to remove certain content posted by minors upon request (the latter is a provision known to privacy law observers as the "eraser button" requirement). *See* Alston & Bird's client alert: *Privacy & Security/Legislative & Public Policy Advisory:* California Establishes Digital Privacy Rights for Minors. Not only does California's new minors privacy law reach well beyond the requirements of the federal children's privacy law, the Children's Online Privacy Protection Act (COPPA), but it has served as a catalyst for privacy legislation introduced in Congress this year to amend COPPA to include similar provisions that would apply to all businesses operating in the United States.

Accordingly, the California AG's guidance to businesses on how to publicly disclose their privacy practices should be evaluated for its potential broader impact on nationwide consumer data collection and disclosure practices. Additionally, businesses should continue to monitor and, where necessary to protect their interests, develop strategies to engage in or address similar privacy legislative developments in Congress and state legislatures that are expected in the months and years ahead.

Dominique R. Shelton | 213.576.1170 | dominique.shelton@alston.com
Paul G. Martino | 202.239.3439 | paul.martino@alston.com

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Kacy McCaffrey
kacy.mccaffrey@alston.com
404.881.4824

Todd S. McClelland
todd.mcclelland@alston.com
404.881.4789

Zachary Neal
zach.neal@alston.com
404.881.4968

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Nicholas Stamos
nick.stamos@alston.com
213.576.2515

Washington, D.C.

Edward Britan
edward.britan@alston.com
202.239.3364

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Paul G. Martino
paul.martino@alston.com
202.239.3439

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jeffrey R. Sural
jeff.sural@alston.com
202.239.3811

ALSTON&BIRD LLP

WWW.ALSTON.COM