Cyberspace LAWYER

June 2014 ■ Volume 19 ■ Issue 5

California AG Kamala Harris Issues Privacy Policy Guidance; Contains Draft Tips for Website and Online Service Privacy Policies

BY DOMINIQUE SHELTON & PAUL MARTINO

Dominique Shelton (dominique.shelton@alston.com) is a partner in the Los Angeles office and Paul Martino (paul.martino@alston.com) is a partners in the Washington, D.C. office of Alston & Bird LLP.

Introduction

California Attorney General Kamala Harris recently released her long-anticipated guidance on privacy policies for companies collecting information from California residents in a report entitled *Making Your Privacy Practices Public* (the "Report"). While the Report exceeds existing law in many respects, affected companies should take heed to review the report and be familiar with its contents as it sets forth a blueprint for how the CA AG's office views "best practices" in connection with privacy policy drafting in the areas of "Big Data," behavioral tracking, data security, and the "readability" of privacy disclosures.

Further, the CA AG takes the position that California's Online Privacy Protection Act (Cal-OPPA) applies to all companies that collect information from California residents – and as such applies to companies operating outside of California.

Key Elements

The key elements of the Report are:

- The Report makes it clear that the plaintiffs' bar should not attempt to use the CA AG's guidance as a sword against companies in over 200 behavioral tracking /Do-Not-Track (DNT) putative class actions pending around

CONTINUED ON PAGE 3

Editorial Board

Cyberspace Lawyer
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ■ 11 Issues ■ $708.88
(ISSN#: 1088-0593)

CONTINUED FROM PAGE 1

the country because the Report states that it is offering "…greater privacy protection than required by existing law" and emphasizes that the recommendations contained in the Report ". . . are not regulations, mandates or legal opinions. Rather, the recommendations are part of an effort to encourage the development of privacy best practices." Further, the CA 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."

- Last year, California enacted a bill, AB 370, which amended Cal-OPPA to require disclosures in privacy policies of how companies' websites respond to behavioral tracking or DNT browser settings selected by online users.[1] Despite AB 370's amendment to Cal-OPPA regarding DNT disclosures, today's guidance from the AG 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." To that end, the Report acknowledges that "[a]s of the end of 2013, the W3C Working Group had not agreed upon what an operator or an advertising network should do when they receive a DNT browser header."
- 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."
- 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." This statement seems to echo some of the statements contained in the two White House reports on Big Data released on May 1, 2014 entitled: (1) "Big Data: Seizing Opportunities, Preserving Values" and (2) "Big Data and Privacy: A Technological Perspective." Links to these reports, which expressed concern regarding the alleged lack of transparency in the collection and creation of Big Data, are in our Alston & Bird's blog post entitled: *The White House Releases Report on Big Data.*[2] Similar sentiments were expressed in the report issued by the Senate Permanent Subcommittee on Investigations on May 15, 2014 entitled "*Online Advertising and Hidden Hazards to Consumer Security and Data Privacy.*"[3]
- The Report recommends disclosing the presence of other parties that collect personally identifiable information on a company's site or service. The CA AG recommends not only that third-party tracking be disclosed as required by Cal. Bus. Professions Code Section 22575(b)(6) (which was newly added by AB 370), but also that companies go above and beyond the law to consider: (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." This recommendation was contained in earlier drafts of the Report circulated in January 2014 to stakeholders.[4]
- The Report furthers the CA AG's focus on improving the "readability" of privacy notices – namely, short clear privacy notices that are not burdened with legalese. Companies are encouraged to consider using a layered notice format, and "[g]raphics or icons can help users easily recognize privacy practices and settings." The identical recommendation was previously made last year in the CA AG's Privacy on the Go report and by the FTC in its mobile privacy guidance. In light of continuing regulatory guidance in this area, 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 icon

program by visiting our web site and viewing our video here.

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."**[1]

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.[2]

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.[3]

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).[4] 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.

---

1. See, 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 for more information about the amendment (http://www.alston.com/advisories/privacy-cal-ab-370/).
2. http://www.alstonprivacy.com/?entry=5293
3. http://www.hsgac.senate.gov/download/report-online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy-may-15-2014
4. For more discussion of the earlier drafts, see Alston & Bird's client alert 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 (http://www.alston.com/advisories/privacy-ab370-dnt-disclosure-best-practice/).
5. *Id.* at 5.
6. *See* Privacy & Data Security Advisory: Special Assistant Attorney General Speaks on Privacy Issues at Alston & Bird's Los Angeles Office. (http://www.alston.com/advisories/attorney-general-privacy-issues/)
7. *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 (http://www.alston.com/advisories/cal-sb-46-breach/).
8. *See* Alston & Bird's client alert: Privacy & Security/Legislative & Public Policy Advisory: California Establishes Digital Privacy Rights for Minors (http://www.alston.com/advisories/privacy-ca-digital-rights-minors/).