California Releases Guidance on DNT Disclosures for Privacy Policies

May 22, 2014

Yesterday, the California Attorney General Kamala Harris released much-anticipated guidance providing website and mobile app operators recommended best practices when disclosing how the operator responds to Do Not Track ("DNT") signals in its online privacy policy.

The guidance, "Making Your Privacy Practices Public," is intended to help companies comply with recent revisions to the California Online Privacy Protection Act ("CalOPPA"), which requires that each privacy policy disclose how the website operator responds to mechanisms, such as DNT signals, that provide consumers with the ability to exercise choice regarding the collection of personally identifiable information ("PII") over time and across third-party websites. In addition to best practices on DNT signals, the guidance also provides general recommendations to make privacy policies "more effective and meaningful" to consumers.

The guidance provides the following 10 key recommendations:

1. ***Scope of Policy***: Privacy policies should explain whether it covers online or offline data collection, or both, and to what entities the privacy policy applies.

2. ***Availability***: A conspicuous link to the privacy policy should be provided on the homepage of the website, and every webpage where PII is collected. For mobile apps, the link should be provided both on the app's platform page and within the app.

3. ***Readability***: Privacy policies should be written in plain, straightforward language that is meaningful to, and can easily be understood by consumers. For smaller screens, such as privacy policies read through mobile apps, the guidance suggests using a layered format that highlights the most relevant privacy issues.

4. ***Data Collection***: Privacy policies should describe how PII is collected (including through the use of cookies or web beacons) and the kind of PII collected. Any information collected from children under the age of 13 should comply with COPPA.

5. ***Do Not Track***: Privacy policies should have a clearly identified section which describes the policy regarding online tracking. A header, such as "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures," can be used to call out the specific section. In addition, privacy policies should describe how the website responds to a browser's DNT signal or similar mechanism. The guidance recommends describing this information in the privacy policy, over linking to a related program or protocol that offers consumers a choice about online tracking.

6. ***Data Use and Sharing***: Privacy policies should explain how PII is used and shared with other

entities, including affiliates and marketing partners, and provide a link to the privacy policies of such third parties.

7. ***Individual Choice and Access***: Privacy policies should describe the choices a consumer has regarding the collection, use, and sharing of his or her personal information
8. ***Security Safeguards***: Privacy policies should explain how the website or app operators protect consumers' PII from unauthorized or illegal access.
9. ***Effective Date***: The effective date of the privacy policy should be provided, and the privacy policy should explain how consumers will be notified about material changes.
10. ***Accountability***: Contact information should also be provided in case consumers have questions or concerns about the privacy policy or practices.