California Attorney General Issues Guidance on Do Not Track

In 2013, the California Legislature passed a tracking transparency bill, AB 370, which amended the California Online Privacy Protection Act ("CalOPPA"). AB 370 requires commercial website operators to inform users of how they respond to the Do Not Track ("DNT") browser signal. Consumers can use the DNT signal to indicate that they do not wish website operators to track their online activities on and between websites. Although consumers can indicate this wish, AB 370 does not require that website operators adhere to the signal by refraining from tracking consumers' online activities. Instead, AB 370 merely requires that website operators inform consumers *how* they respond to the DNT signal.

This left stakeholders at a loss as to how exactly to comply with the new DNT disclosure requirement. In response to this ambiguity, the California Attorney General Kamala Harris ("CA AG") issued a guidance entitled *Making Your Privacy Practices Public* (the "Guidance") on May 21, 2014.

Legal Framework of Do Not Track

Generally, CalOPPA regulates how commercial website operators and online services collect, store, and share personally identifiable information ("PII") of Californians. It requires commercial website operators to conspicuously post privacy policies informing users of how and why they and third parties will use PII. Many website operators question why they ought to adhere to CalOPPA. The answer is that the combination of California's robust economic presence and the interconnectivity of the web means CalOPPA affects most commercial website operators. The CA AG can bring enforcement actions against website operators who violate CalOPPA, and has shown a willingness to reach broadly.

Additionally, the FTC has brought a number of actions against companies claiming that misstatements in privacy policies are unfair trade practices under Section 5 of the FTC Act. In 2010, the FTC endorsed the DNT signal as a uniform way for users to choose whether commercial website operators could collect information about their online searching and browsing activities. The White House echoed this in its 2012 report entitled, *Consumer Data Privacy in a Networked World*, which stated, "privacy-enhancing technologies such as the 'Do Not Track' mechanism allow consumers to exercise some control over how third parties use personal data or whether they receive it at all." To date, there has been no public action brought by the FTC regarding a company's DNT signal disclosure, though the potential for it doing so is another reason for caution.

The CA AG's recent Guidance recommends website operators do the following to comply with AB 370:

- Devote a section of the privacy policy to DNT, entitled "How we respond to Do Not Track Signals," "Online Tracking," or "California Do Not Track Disclosures."
- Describe the website operator's response to DNT or other mechanism.
- Also describe, including whether the website operator actually honors DNT.
- If the website operator does not honor DNT, then provide a "clear and conspicuous link to a program that offers consumers a choice about online tracking."
- Disclose presence of other parties that collect PII on website operator's site or service.
- Confirm that privacy policy disclosures reflect the website's actual DNT practices.

What Do "Best Practices" Mean?

Some stakeholders have questioned whether the CA AG's "best practices" and "recommendations" carry the force of law. They ask whether website operators face regulatory actions if they do not follow the CA AG's recommendations, and conversely, whether following the CA AG's recommendations will protect them from regulatory action or litigation. In response, the CA AG stated in issuing the Guidance that her recommendations in them "in some places offer ***greater privacy protection than required by existing law, are not regulations, mandates or legal opinions***." It remains unclear how this statement will affect regulatory action and litigation.

While CalOPPA does not provide for a private right of action, the CA AG can bring enforcement actions under the law. Violations of CalOPPA may result in penalties of $2,500 per violation. Therefore, website operators should take heed of the CA AG's Guidance on DNT and update their privacy notices accordingly.

Is the Consent Model Still Valid?

The Guidance indicates the CA AG is reinforcing the approach of earlier privacy frameworks, which focused on trying to achieve consumer transparency and consent. However, the White House issued two reports this month, both of which indicate a desire to move away from the consumer consent model and towards more direct governmental regulation of data use. This is being recommended in large part in recognition that the transparency and consent regulatory model is ineffective. For instance, the May 2014 Report to the President entitled *Big Data and Privacy: A Technological Perspective*, remarked that "***[o]nly in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent***." It remains to be seen whether the notice and consent model is being taken to a potentially formalistic high with AB 370 (to be followed by other governments), or whether states and Washington will begin to meaningfully turn their focus to how data is used by different businesses. For the time being, the requirements of AB 370 are on the books and apply to most website operators. For more information, feel free to contact Jim DeGraw, Debbie Gersh, Tim McCrystal, Dave McIntosh, Doug Meal, Mark Szpak, Michelle Visser, Claire Lucy Readhead or any other member of our leading privacy & data security practice team.