THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Angelique Carson, CIPP/US

June 2014

FEATURE STORY

Unpacking the California AG's Guide on CalOPPA

By Lei Shen, CIPP/US

Determining how to comply with California's "Do Not Track" requirements has been a challenge. The amendment to the California Online Privacy Protection Act (CalOPPA) became effective on January 1 and began requiring privacy policies to include certain Do Not Track (DNT) disclosures. However, there has been some uncertainty as to how to comply. Because DNT is not a finalized standard, it is unclear what even qualifies as a DNT signal under CalOPPA. In addition, different browsers implement their Do Not Track mechanisms differently—some set it as the default setting, while others require the user to configure it—so it's difficult to determine what the user's actual expectation is.

In an effort to curb this uncertainty, the California Attorney General (AG) recently released a guide titled *Making Your Privacy Practices Public*. The guide provides long-awaited guidance on how to comply with the CalOPPA Do Not Track requirements, among other recommendations. The AG, Kamala Harris, stated that the guide is intended to provide a "tool for businesses to create clear and transparent privacy policies that reflect the state's privacy laws and allow consumers to make informed decisions."

While the guide provides recommendations on how to comply with CalOPPA, they are not legally binding. In fact, several of the Guide's recommendations going beyond the requirements of CalOPPA. This article summarizes the Guide's recommendations and compares them to CalOPPA's actual requirements.

Online Tracking and Do Not Track

The CalOPPA amendment added two tracking disclosure requirements for privacy policies. First, website operators must disclose in their privacy policies how they respond to web browser "do not track" signals or to similar technologies that provide users with an ability to exercise choice regarding tracking. CalOPPA does not require a website to respond to such signals, but simply disclose how it responds. An alternative way for a website operator to comply is to provide a "clear and conspicuous hyperlink" in its privacy policy to an online location containing a description and the effects of a program or protocol that the operator follows that offers users a choice regarding online tracking. Second, in addition to the Do Not Track disclosure, CalOPPA also requires that privacy policies disclose whether third parties conduct tracking on the website.

The guide's recommendations go beyond these CalOPPA requirements in a number of ways. For instance, CalOPPA only requires that these tracking disclosures be included somewhere in the privacy policy. A number of

website operators have been complying by including the disclosures within other similar provisions. However, the guide recommends that these disclosures be clearly identified with their own header in the privacy policy, such as "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures."

If a website follows a consumer-tracking choice program or protocol, CalOPPA permits compliance with the Do Not Track disclosure requirement by including a link to a description of that program or protocol within the privacy policy.

However, the guide recommends that, in addition to the link, the privacy policy also provide either a description of the website's response to Do Not Track signals or a brief, general description of the applicable program or protocol and what it does, to provide greater transparency to consumers. The guide also recommends that the disclosure describe whether the website treats consumers whose browsers send a Do Not Track signal differently from those that do not.

It also recommends that the disclosure describe whether the website still tracks even if it receives a Do Not Track signal, and if so, how that information is then used.

Availability

CalOPPA requires that a privacy policy be "conspicuously posted" on a website. A privacy policy can be "conspicuously posted" if the website's home page contains an icon or text link that includes the word "privacy" and is linked to the privacy policy. Another way a privacy policy can be "conspicuously posted" is if the text link to the privacy policy is either written in capital letters that are at least the same size as the surrounding text or is otherwise written in way that calls attention to the link (e.g., written in a larger type than the surrounding text, in a contrasting type, font or color, or set off from the surrounding text by symbols or other marks).

The guide recommends that, in addition to these requirements, a website also include a link to the privacy policy on every webpage where personal information is collected. For online services, such as mobile applications, the privacy policy should also be posted or linked to on the application's platform page so that users can review the privacy policy before downloading the application as well as from within the application.

Readability

While CalOPPA does not have any requirements regarding readability, the guide reiterates prior guidance regarding readability from the Federal Trade Commission (FTC) and the California AG. For example, a privacy policy should be formatted in a way that makes it readable, especially on smaller screens like a mobile device. One such format is a layered format that highlights the most relevant privacy issues. Websites can also use graphics and icons in their privacy policies to help users more easily recognize privacy practices and settings.

Data Collection, Use and Sharing

CalOPPA requires that a privacy policy identify both the categories of personal information that a website collects and the categories of third-party persons or entities with whom the website operator may share that personal information.

The guide recommends that a privacy policy go beyond merely identifying general categories by being reasonably specific about the kinds of personal information being collected and identifying the retention period for each. In addition, a privacy policy should generally describe how a website collects personal information, including

specifying if any information is collected from other sources (e.g., offline or from third parties) or through technologies such as cookies or web beacons.

If a website collects any personal information from children under the age of 13, the guide cautions that the Children's Online Privacy Protection Act (COPPA) has additional obligations for the website operator, including the requirement to obtain verifiable parental consent prior to collecting any information from children.

With regard to sharing, the guide clarifies that when a privacy policy describes the different types of third parties with which the website operator shares personal information, affiliates and marketing partners should be mentioned if applicable and links to the privacy policies of those third parties should be included.

Lastly, if a website uses personal information beyond what is necessary for fulfilling a transaction or providing an online service, the privacy policy should explain this.

Individual Choice and Access

If a website operator maintains a process for an individual to review and request changes to his or her personal information that was collected through the website, CalOPPA requires that the privacy policy provide a description of that process.

The guide expands on this by recommending that a privacy policy also describe any choices an individual may have regarding the collection, use and sharing of his or her personal information, rather than limiting that process to the review and correction of that personal information.

In addition, if an individual requests to review or correct his or her personal information, then the website operator should first ensure that the individual's identity is properly verified and any access rights are authenticated.

Security Safeguards and Accountability

CalOPPA does not require that a privacy policy explain the website's security safeguards or provide a contact for questions. The guide, however, recommends that a privacy policy explain how the website protects its users' information from unauthorized or illegal access, as well as provide contact information if users have any questions. It is important that the security statements do not misrepresent or "over-promise" the website's actual security, as the FTC has been taking action against companies that do not live up to their security promises.

While much of the guide is not mandatory, its recommendations reiterate and align with several of the key recommendations from other similar publications, including those from the FTC, and provide a good basis for companies to use when drafting or revising their privacy policies to provide more transparency to users.

Lei Shen, CIPP/US, *is a senior associate in the Business & Technology Sourcing practice in Mayer Brown's Chicago office. She focuses her practice on privacy and security, technology and business process outsourcing, and information technology transactions. Lei can be reached at lshen@mayerbrown.com.*

.