Foster Garvey

Duff on Hospitality Law

California Adds "Do Not Track" Disclosure Requirement to the California Online Privacy Protection Act

By Greg Duff on 2.20.14 | Posted in Data Privacy

In September, 2013, Governor Jerry Brown of California signed into law Assembly Bill No. 370, which amends the California Online Privacy Protection Act (CalOPPA) to require that website and mobile app operators disclose whether they honor web browser "Do Not Track" signals. AB 370 took effect on January 1, 2014.

CalOPPA

CalOPPA has, since 2003, required operators of commercial websites or online services that collect personally identifiable information (PII) from California consumers (including, most notably, guests and customers from California) through the Internet to post, conspicuously, their privacy policies. PII is "identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form." PII includes, but is not limited to, first and last names, home or other physical addresses, email addresses, telephone numbers, social security numbers, and any other identifier that permits the online or physical contacting of a specific individual. PII also includes "[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."

CalOPPA requires privacy policies to make certain specific disclosures regarding how the website or app operator collects, uses, and discloses users' PII. For example, operators must disclose the type(s) of data they collect and the categories of third parties with whom that information is shared, if any. In addition, privacy policies must provide an effective date, information regarding how a consumer can access and/or request changes to his or her PII, and a description of how the operator will notify consumers of policy changes.

Operators are in violation of CalOPPA if they knowingly and willfully, or negligently and materially fail to comply with either the law or the operator's own privacy policy. Violators can incur a civil fine of up to $2,500 per violation. Importantly, the California Attorney General maintains that *each* non-compliant mobile app download constitutes a violation, which may trigger the fine.

Do Not Track and AB 370

Do Not Track (DNT) mechanisms typically are small pieces of code, similar to cookies, that signal to websites and mobile applications that the user does not want his or her website or app activities to be tracked. Most Internet browsers, including Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, and Apple Safari, allow users to choose whether to have the browser send out DNT signals. If a website that honors DNT signals receives such a signal, the browser blocks the website from collecting PII from that user.

AB 370 amends CalOPPA to require covered operators to update their privacy policies to include new disclosures. Specifically, the amended Act now requires that operators disclose:

- How they respond to DNT signals or other mechanisms that allow consumers to choose whether and how PII about their online activities is collected over time, both by the operator and across third-party websites or online services; and
- Whether third parties may collect such PII over time and across different websites when the consumer uses the operator's website or service. However, the operator need not disclose the identities of such third parties.

AB 370 **does not** require website and app operators to obey DNT signals—it merely requires that operators disclose whether they obey or do not obey such signals. Operators may satisfy this requirement by either, if they do not respond to DNT signals, stating as much in their privacy policies, or, if they do respond to DNT signals, including in their policies a description of the program or protocol they use in responding or a clear and conspicuous hyperlink to an online location containing such a description.

Recommendations

Hoteliers and restaurateurs that operate websites, mobile applications, or other online services that collect personal information from California residents should familiarize themselves with both CalOPPA and AB 370. In addition, operators should review their websites and apps to determine how they respond to DNT signals and the tracking methods they use, as well as whether third parties (e.g. vendors or suppliers) conduct tracking activities on or using their websites or apps. Hoteliers and restaurateurs should then revise or update their privacy policies as needed.

Hoteliers and restaurateurs should be aware that other state laws and/or federal laws such as the Healthcare Information Portability and Accountability Act (HIPPA) or the Children's Online Privacy Protection Act (COPPA) may also apply, depending on what information the Hotelier or restaurateur collects and from whom.

Please contact Greg if you have further questions regarding CalOPPA or any other privacy matter.

Tags: CalOPPA, DNT, Do Not Track and AB 370