Hughes Hubbard & Reed

California Continues Campaign Against Online Tracking

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

As we've previously discussed, the State of California's new amendment to the California Online Privacy Protection Act ("CalOPPA") took effect on January 1, 2014. One key component of this new iteration of the statute is the requirement of website operators to disclose how they respond to web browser "do not track" ("DNT") signals or other similar mechanisms that provide a consumer with the ability to exercise choice over the collection of personally identifiable information ("PII"), including information about that consumer's online activities over time and across third party websites or other online services. It may not affect a website's ability to track internally, use third party analytic services, or track basedon information that doesn't include PII (such as IP addresses), but the new disclosure requirements are still burdensome.

Website operators that do not comply with CalOPPA will be issued a 30-day warning/grace period to modify their practices to ensure compliance. The California Attorney General's Office recently published guidelines to assist website operators with their compliance efforts. Although not technically binding, the guidelines reveal changing expectations regarding online privacy and, in light of the California AttorneyGeneral's aggressive stance on compliance monitoring and enforcement, allwebsite operators should take notice of what has been deemed acceptable conductunder CalOPPA.

The key elements of such guidelines are as follows:

- Website operators should clearly identify the section of their privacy policies that cover online tracking and DNT signals. The California Attorney General's mission is to make it simple for consumers to find this section of privacy policies since consumers whose browsers send DNT signals cannot otherwise easily determine how a website or service responds to the signals.
- Website operators should describe how they respond to DNT signals. The guidelines suggest that this is preferable to simply linking to a program that offers a consumer a choice about tracking in the absence of such description. The California Attorney General's commentary also suggests specifying (1) if treatment of consumers whose browser sends a DNT signal is any different from those whose browser does not and (2) if PII is still collected over time and across third party websites or other online services despite a consumer's

browser sending a DNT signal. If PII is collected despite a DNT signal, the guidelines recommend that website operators describe how such information is used.

- If there is no description of how a website operator responds to a DNT signal, then such website operator should provide a "clear and conspicuous" link in its privacy policy to a program offering consumers a choice about online tracking. The linked page should make clear what a consumer must do to make the choice and include a clear statement about the program's effects on the consumer, such as whether any PII will still be collected if the consumer chooses not to participate.
- Website operators should disclose whether any other parties track consumers and collect PII while consumers are using their website. This statement as to other parties should cover (1) whether the website operator has approved all third party collectors, (2) how the website operator verifies that approved third party collectors are not driving other, unauthorized collectors to the website and (3) how the website operator confirms that third party collectors comply with the website operator's privacy policy, including its DNT policy (or, if confirmation is not possible, the website operator should include a disclosure that third party collectors may not comply with the website operator's privacy policy).

These guidelines present new challenges for website operators. Describing current PII collection mechanisms may seem rudimentary at first blush, but given the wide variety of browsers and websites and their respective functionality, disclosing such mechanisms in sufficient detail requires a thorough understanding of both the features employed by the latest versions of browsers and the technical/operational characteristics of DNT signals. These descriptions will need to be regularly updated as well, adding another layer of complexity to website operators' compliance efforts. Indeed the lack of consensus among browser developers and website operators on how to send out and respond to DNT signals lends strong support for the notion that a fulsome disclosure should invariably account for any new standards or features that may be developed and employed in the future, such as new anti-tracking tools.

Website operators may find themselves on the wrong side of a claim asserted by opportunistic plaintiffs attempting to capitalize on a new type of DNT signal or some widely perceived ambiguity in the law. Therefore, it is critical for operators of websites and other online services to review their privacy practices and policies immediately in order to assess whether revisions are necessary in order to comply with this latest amendment to CalOPPA. It is also highly recommended that website operators closely monitor and scrutinize novel DNT signal developments such as the World Wide Web Consortium's Tracking Protection Working Group's call for comments on a newly proposed definition of DNTsignals. The DigitalHHR team will continue to monitor the latest developments surrounding CalOPPA and online privacy issues generally. Please feel free to reach out to us with any questions or concerns.

Related Areas of Focus

Media, Technology & Commercial Transactions