Hughes Hubbard & Reed

Privacy Alert – Amendments to CalOPPA in Effect as of January 1, 2014 – Have you Reviewed Your Privacy Policy?

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

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. For information regarding the selection process of awards, please visit https://www.hugheshubbard.com/legal-notices-methodologies.

On September 27, 2013, the State of California enacted Assembly Bill No. 370("AB370"), amending the California Online Privacy Protection Act ("CalOPPA"). CalOPPA requires any operator of a commercial website or online service provider that collects personally identifiable information ("PII") from any individual residing in California (collectively, "operators"), whether through a website, mobile application or otherwise, to conspicuously post a privacy policy and comply with such privacy policy. Prior to the passage of AB370, CalOPPA required that such privacy policy disclose the following:

1. A description of the categories of PII that the operator collects, as well as the categories of third parties with whom such PII may be shared;
2. A description of the process maintained by the operator that allows an end user to review and request changes to any of his or her PII that is collected;
3. A description of the process maintained by the operator for notifying an end user of any material changes to its privacy policy; and
4. The effective date of the operator's privacy policy.

Additional Disclosures Required by AB370

In addition to the disclosures set forth above, AB370 introduces the following disclosure obligations for operators:

1. To the extent that an operator engages in the collection of PII about an individual's online activities over time and across third party websites or online services, such operator must disclose how it responds to web browser "do not track" ("DNT") signals or other mechanisms that provide consumers with the ability to exercise choice regarding the collection of such PII; and

2. An operator must disclose whether third parties may collect PII about an individual over time and across different websites when an individual uses the operator's website or online service.

What it Means for You

The State of California has previously taken the position that operators that fail to comply with the requirements of CalOPPA will be issued a warning, coupled with a 30-day cure period in which to comply. Those operators failing to comply with such requirements within such 30-day period will be deemed in violation and may be fined heavily under California's Unfair Competition Law.

Compliance with these new disclosure requirements poses significant challenges to operators. Despite the efforts of industry groups such as the World Wide Web Consortium's Tracking ProtectionWorking Group, no clear industry standard has yet to be established in order to guide operators in their identification of and response to DNT signals or other mechanisms now regulated under CalOPPA. Additionally, the lack of standard protocols transcends further to the actual technology. For example, although web browsers have now generally implemented DNT functionality for end users, these features vary from browser to browser, further complicating operators' compliance efforts.

The DigitalHHR team has received numerous inquires regarding the implications of AB370 and continues to monitor the latest developments surrounding this constantly evolving discussion. Despite the uncertainty, operators of websites and online services should review their privacy practices and policies immediately in order to assess whether revisions are necessary in order to comply with AB370. If you have any questions, please feel free to reach out to us.

Related Areas of Focus

Media, Technology & Commercial Transactions