KILPATRICK TOWNSEND

Insights: Alerts

Your Company's Website Privacy Policy Probably Needs a Refresh (Before February 1, 2017)

January 9, 2017

Written by **Barry M. Benjamin, Amanda M. Witt, Jon Neiditz** and **Michelle Tyde**

As 2016 has come to a close, now is a good time to take stock of new disclosure obligations for website privacy policies introduced over the course of the year. It is likely that if your company's privacy policy has not been updated in some time, it could use some refreshing. The questions below will help you to review your privacy policy and identify any areas that need updating.

Does Your Privacy Policy Comply with the new Delaware Privacy Law?

The Delaware Online Privacy and Protection Act ("DOPPA") came into effect at the beginning of 2016. The law (substantially similar to California's Online Privacy Protection Act) requires a number of things, both in the content of a privacy policy and how links to it are disclosed. In terms of content, DOPPA requires a company privacy policy to state how the website handles "do not track" requests, to detail the categories of personally identifiable information the company collects, and to list the categories of third parties with which personally identifiable information are shared. Links to the privacy policy both online and on mobile devices must be "conspicuously" posted, by including a direct, clear hyperlink to the policy. .This likely means that if your website does not provide a direct 'privacy policy' link, but rather includes the privacy policy in a link called 'legal' or other words to that effect that do not reference 'privacy' specifically, give consideration to altering the language used in the link.

Does Your Company Engage in Cross-Device Tracking and Comply with DAA Guidance?

The Digital Advertising Alliance (DAA) is a self-regulatory body that oversees online interest-based advertising. Over the years, it has issued principles and guidance to which companies in the online interest-based advertising eco-system must adhere. The DAA also set up an accountability program to oversee and ensure compliance with those principles and guidance.

In late 2016, the DAA announced that it will commence enforcement of its guidance with respect to cross-device tracking, on February 1, 2017. The cross-device tracking guidance requires companies to provide disclosure and transparency about how they track users across their multiple devices, by notifying users in the company's privacy policy about the company's practices. This includes providing notice to users of the fact that cross-device tracking is taking place, as well as notice to users about how they can opt out of cross-device tracking. Importantly, and a point not necessarily obvious, is that the DAA's guidance requires companies to

honor a user's opt out exercised on a single device, across the user's many devices. This means that companies must implement technologies to prevent data collected on a particular browser or single device, on which the user's opt out choice is exercised, from being used on another computer or device that is linked with that user's browser or device.

The upcoming enforcement will not only impact DAA participants, but will also affect companies that contract with participants. Vendors that perform data analytics or provide advertising services frequently participate in the DAA and often contractually require their customers to comply with DAA Principles. For more information see: Enforcement of DAA Cross Device Tracking Guidance Set to Begin in Early 2017.

Does Your Website Use Google Analytics?

Also in 2016, Google updated its policies with respect to its Analytics products. The updated policy requires website operators that use Google Analytics to disclose three things in their privacy policies. First, the policy must specifically list the Google Analytics advertising features that the website operator has implemented, instead of generically citing the use generally of Google Analytics as a whole. Second, the policy must describe how the website operator and its third party vendors use first-party cookies or identifiers together with third-party cookies. Third, the policy must include an opt-out section for the specific Google Analytics features the website operator has implemented, whether that is through a setting or through a broad opt-out such as the consumer opt-out provided by the NAI. Google also encourages, but does not require, websites to direct their users to Google Analytics' opt-out for the web.

Will Your Company be Self-Certifying to the EU/U.S. Privacy Shield?

If your company is considering self-certifying to the Privacy Shield Framework, it is essential to review the company's privacy policy and make any necessary updates to ensure the policy is Privacy Shield-compliant, or to create prepare a separate Privacy Shield Privacy Notice. For example, the Privacy Shield Privacy Policy must:

- Be clear, concise and easy to understand;
- Describe the Company's information handling practices and the choices the Company offers individuals with respect to the use and disclosure of their personal data;
- Specifically refer to the Company's Privacy Shield compliance, and provide a hyperlink to the Department of Commerce's Privacy Shield website;
- Identify the Company's independent recourse mechanism, and provide a hyperlink to the website of the recourse mechanism or to the independent recourse mechanism's complaint submission form;
- Include a statement of the individual's right to access his or her personal data;
- Identify the statutory body that has jurisdiction to hear claims against the Company; and
- Explain that the Company may have a requirement to disclose personal data in response to lawful requests by public authorities, including to meet national security requirements.

If you have any questions or concerns about these requirements or about privacy compliance in general, please feel free to reach out to us. Kilpatrick Townsend's Cybersecurity and Privacy team is deeply committed to helping its clients integrate their privacy programs into their business strategies, addressing their bigger marketing, customer relations, and risk management issues along with regulatory compliance.

Related People

Barry M. Benjamin

Partner
New York, NY
t 212.775.8783
bbenjamin@kilpatricktownsend.com

Amanda M. Witt

Partner
Atlanta, GA
t 404.815.6008
awitt@kilpatricktownsend.com

Jon Neiditz

Partner
Atlanta, GA
t 404.815.6004
jneiditz@kilpatricktownsend.com

Michelle Tyde

Counsel
Atlanta, GA
t 404.815.6001
mtyde@kilpatricktownsend.com