AMERICAN MARKETER

Business at its best

COLUMNS

One year after the Digital Advertising Alliance's mobile privacy guidance

August 30, 2016

Lou Mastria is managing director of the Digital Advertising Alliance

By Lou Mastria

The traditional first anniversary gift is paper, but as the Digital Advertising Alliance (DAA) marks the first anniversary of its enforcement deadline for its mobile privacy guidance on Sept. 1, a more appropriate symbol might be steel, as the program has built a solid infrastructure of independent enforcement, with numerous investigations and public actions against companies in violation of that guidance.

The actions taken since then provide both a warning and a roadmap for other marketers on how to ensure that they are in full compliance with their privacy obligations in the mobile space.

Guidance

As this publication's readers will recall, the DAA unveiled its guidance for the application of the DAA's self-regulatory principles in the mobile environment three years ago.

The guidance explained how companies should provide notice and choice in the mobile environment, including the appropriate use of the mobile YourAdChoices icon and new AppChoices app.

The guidance also extended the application of other DAA principles around the use of sensitive information, and it explained the enhanced notice and choice needed to collect and use of precise location and personal directory data for interest-based advertising.

Notably, the guidance made clear that data collection and use practices in the mobile environment fell under the existing enforcement regime of the DAA's accountability programs, run by the Council of Better Business Bureaus (CBBB) and the Direct Marketing Association (DMA).

The DAA's enforcement partners have broad authority to investigate and engage with companies whose products or services are not in compliance with the DAA Principles and work with them to resolve any violations. They can also refer companies in violation to the Federal Trade Commission or other regulatory agencies for additional action, as needed.

Following the release of the mobile guidance, the DAA set an enforcement deadline of Sept. 1, 2015.

To ensure that companies understood their new responsibilities, the DAA and its enforcement partners undertook an aggressive industry education campaign in the period leading up to the deadline, including webinars, industry events and one-on-one consultations.

While most companies quickly came into full compliance, the DAA's enforcement partners have been forced to take public action against several that did not.

public action against several that did not.

Lessons

In the last three months, the CBBB's Online Interest-Based Advertising Accountability Program has released information on those actions against five companies for their violations.

Two of the actions were related to insufficient notice and choice being provided to consumers around the collection of precise location data for use in interest-based advertising, two involved failures to meet the heightened responsibilities for applications that are designed to appeal to children under age 13, and one covered both of those issues, as well as a general failure by the app to provide transparency and consumer choice to mobile users.

All five of the companies named in the public actions have taken remediation steps in consultation with the CBBB to address the issues raised and move their mobile apps into compliance with the mobile guidance.

What lessons can be learned from their experience?

First, it is vital for every company to review its mobile policies and practices including the real-world behavior of its mobile apps and properties to ensure that they are in compliance.

If a company has questions or concerns, it can reach out directly to the CBBB or DMA without repercussions to better understand their obligations and the steps it needs to take.

Next, location data and children's privacy are areas that require special attention and review.

In both cases, the behavior of mobile apps and properties may vary significantly from the desktop experience, and violations risk action not only by the DAA's enforcement partners, but also from the FTC or other regulatory agencies.

Finally, technologies change rapidly, and mobile services go through continuous iterative upgrades, so a one-time audit or review is not sufficient to ensure a company's products remain in compliance.

A company must conduct ongoing or, at least, regular examinations of its privacy practices in the mobile environment to maintain its clean bill of health.

BY INSTITUTIONALIZING these simple privacy steps, mobile technology companies can continue to push the leading edge of innovation and provide next-generation services to consumers without risk of negative industry or regulatory action.

Lou Mastria is managing director of the Digital Advertising Alliance, New York. Reach him at lou@aboutads.info.