February 27, 2017

CROSS-DEVICE TRACKING AND CONSUMER PROTECTION: IS THERE MORE TO THE STORY?

by Vejay G. Lalla

In 2017, we are seeing an explosion of online marketers engaging in cross-device targeting, where data is used to identify users on one device to serve ads to them on a different device. This enables advertisers to pinpoint their consumers as never before.

Now, they can capitalize on key moments of a consumer's purchasing journey to keep the consumer engaged and, more importantly, to piggyback on those purchases. For example, a consumer purchasing a department store dress on her laptop may be seamlessly served an ad for matching shoes on her smartphone only a few minutes later.

The regulators are keeping a close eye on these developments. The Federal Trade Commission (FTC) recently issued a new staff report on cross-device tracking and, days later, the Digital Advertising Alliance (DAA) began officially enforcing its cross-device privacy rules.

But there is more to the story: Managing a seamless cross-technology program presents unique challenges to marketers who are running advertising campaigns on multiple platforms and using multiple vendors to do so. These campaigns are no longer siloed, which means that advertisers need to keep in mind traditional advertising and consumer protection principles alongside the emerging privacy implications.

TWIN PILLARS: TRANSPARENCY AND CHOICE

In recent reports and associated guidance, the DAA and the FTC have identified the benefits and challenges of cross-device tracking. These regulatory bodies continue to emphasize that marketers must keep key principles of transparency and choice in mind when developing and implementing data security practices for cross-device data.

While tracking such information can improve the consumer experience and enable companies to build detailed consumer profiles, these companies may get themselves into hot water if they do not appropriately disclose tracking to their consumers and business partners and give these third parties choices about how their activity is tracked.

Now, the most successful marketers are feeding online and offline data, such as catalog responses and brick-and-mortar rewards program participation, into their cross-device strategies to build a better understanding of how to generate value across their consumer bases and more accurately identify their targets. But the FTC has pointed out in its staff report that many consumers may be unaware that tracking extends to physical retail locations, "smart" in-home devices or wearable technology, as opposed to just their laptops and smartphones.

In addition, the amount of data being collected and analyzed by these companies can be staggering and, especially in cases where sensitive data such as geolocation, health information, financial information or data of minors is involved, may merit special security policies and procedures.

LOOKING BEYOND PRIVACY

In light of these concerns, compliance with the recent DAA and FTC guidance is certainly paramount. But there is even more at stake when managing these types of campaigns, and keeping tabs on consumers and developing custom advertising implicates more than just privacy laws.

In a world where a single company may delegate any or all elements of its integrated marketing programs to different vendors, publishers or technology tools, it is becoming ever more important for marketers and their agencies to have a ground-up, holistic compliance and contracting strategy to cover all their legal bases, particularly since marketers work with a range of vendors.

While a marketer may use one vendor to scrape purchasing data from a website and match it with a consumer profile, for example, another creative agency may be responsible for producing native and targeted content to be served to that consumer on another platform. Yet another company or publisher partner may be responsible for buying ad space online and placing the content.

While the first vendor would be responsible for collecting and hosting the data in compliance with the applicable laws and security standards, the creative agency may be responsible for clearing third-party rights in native ads and custom content, while the publishers and media-buying partners need to consider disclosures required by regulators and ownership or other intellectual property issues.

As such, it is the advertiser's responsibility to ensure that it is developing a compliance program that takes into accounts all facets of the advertising journey – not just the data that generates it.

Even if a marketer can pin blame on one of its vendors from a contractual standpoint, unless there is a data breach caused by the failure of a vendor's security practices, regulators are more than ever focused on the brand that is controlling and approving the levers of these programs than each of its technology partners. Ultimately, in a world where advertising has become fluid, marketers can no longer treat each of these relationships as a separate deal.