How Cookie-Syncing Works

Oct 16th 2020

There is a common misconception that all cookies are bad and violate user privacy. However, some types of cookies (first-party cookies) are created by the websites we visit directly, and serve to actually improve a website's user experience. Third-party cookies on the other hand are created by advertisers for the purpose of tracking and data collection, including data passed on from the website visited, such as the user's interests, location, and age. They also track a user's behavior, such as the content they view on the publisher's site and the things they click on (e.g. products and ads).

The big limitation of cookies in general is that they can only be read on the domain that created them. This means that AdTech companies can't read cookies created by other AdTech platforms or by the website itself, essentially limiting their effectiveness for advertising purposes on other websites. To better understand this problem, consider that demand-side platforms (DSPs) and data management platforms (DMPs) are 2 common components of the AdTech ecosystem. DSPs allow advertisers at a brand or an advertising agency, to buy ad impressions programmatically in real time from ad exchanges. DMPs are used to import data from various sources, create user profiles containing valuable attributes (such as age, location, interests, web browsing history, and more), and build audience segments. In order for the advertiser to enhance their targeting capabilities and increase the potential value of each impression, the DSP and DMP must overcome the domain limitation aspect through a process called cookie syncing.

In this process, the DSP that receives the initial ad request, redirects the browser to its associated DMP alongwith the DSP's ID for the user by way of a transparent 1x1 pixel. The DMP in turn stores the DSP ID into a cookie matching table, together with its own identifier. With cookie syncing established, whenever the DSP and DMP want to exchange information, they have a common basis of identifying the individual being targeted. Note that while the cookie-syncing process of requests and redirects between the browser, DSP, and DMP happens in real time, the actual sharing of user data might happen once a day at a certain time. Data sharing is typically done via a server-to-server integration with the data being transferred in large batch files.

Cookie syncing is only performed in web browsers, whether that be desktop or mobile web browsers. ==Native mobile apps use the device's Advertising ID (IDFA & AAID) as a way to identify users==.

Source : ClearCode Article, AWS Article,