Ad Tech & Ed Tech Call 1: Ad Tech 101

Friday, June 30, 2017
Time: 11:30am-12:30pm

Brian Nixon (Loeb & Loeb) on the Ad-Tech Landscape

The Evolving Advertising Landscape

- Advertising and marking is increasingly involving the collection and use of data.
- The sources of this data can vary and may be gathered from news, social media, census data and many others.
- This data is used to make informed decisions in marketing, product development, and other business functions.

Examples of Data Driven Advertising

- Some examples of how data is being used to inform advertising:
    1. Through the use of cookies (small data files stored on a user's computer) and other tracking technologies, website publishers and other third parties are able to track a significant amount of information about how websites are being used. This information allows advertisements to be served based upon a user's prior browsing activity. This is called interested-based advertising.
    2. One of the most basic forms of target advertising is "keyword advertising." In "keyword advertising" a user's keyword searches triggers the display of advertisements relevant to those particular keywords.
    3. Another type of advertising using data is contextual advertising. Contextual advertising refers to advertising based on the content of the website a user visits.
    4. First party targeting advertising is yet another example of data driven advertising. This occurs when the owner or operator of a website offers products or services based on the user's previous actions on the website through the use of cookies.
    5. In behavioral or interest-based advertising, the advertiser or advertisement server builds a profile on the user's browsing history across multiple websites.
    6. A final example of this data driven advertising is retargeting advertising. This enables advertisers to remarket their products to previous buyers. This works by placing a pixel on the advertiser's website. Every time a new visitor goes to the advertiser's website, the pixel places a cookie on the visitor's browser. When the visitor leaves the website, the cookie notifies advertisers that the visitor should be retargeted with advertisements from the previous website.

Facebook's Custom Audiences

- There are many types of vendors that enable targeting advertisements.
- One particularly popular vendor used in this industry is Facebook's custom audiences.
- This enables advertisers to match data that they have about their existing customers with Facebook user information to deliver targeted ads.

- The Facebook custom audiences match could be based on a customer's email, phone number, Facebook unique identifier, or a mobile advertising ID.
- This type of targeting advertising can be based on the use of an app on a mobile device which can be used to encourage mobile users to return to an advertiser and purchase items left in their virtual shopping cart.
- Mobile apps can be configured to be left on and collect vast amounts of information about a user such as communications with a user's contacts, photos and videos, geolocation information, and web browser information.

Beacon Use by Retailers

- Retailers are increasingly using beacon technology to serve advertisements to customers.
- Beacons are wireless sensors and transmitters that deliver targeted offers and services when consumers are in or near their stores.
- For example, sports stadiums use beacons to welcome patrons as they walk through the entrance to their venue and to send them custom offers as they are at the event.
- Apple's iBeacon can go so far as to identify which isle of a supermarket a user is in.

Targeted Advertising Campaigns

- Targeted advertising campaigns are increasingly being executed through the use of programmatic buying of advertisements. This entails a wide range of technology. It automates the buying, placement, and optimization of ads.
- Real-time bidding is a type of programmatic buying and is generally used for on-line display advertisements, mobile video, television, and out of home advertisements.

Advertising Self-Regulation

- The Digital Advertising Alliance (DAA) manages a self-regulatory program for online and mobile advertising as well as cross-device advertising.
- The DAA requires enhanced notice on every webpage that collects data for interest-based advertising.
- The DAA also requires websites using interest-based advertising data to provide consumers with an easy to use opt-out mechanism.
- The DAA licenses the "Ad-Choice Icon" which is often displayed on online advertisements to illustrate compliance with DAA principles.

Susan Isreal (Loeb & Loeb) on the Ad-Tech 101

Additional Targeted Advertisement Self-Regulation

- There is an additional internal self-regulatory organization called the Network Advertising Initiative (NAI).
- NAI represents mostly the companies that don't interact directly with consumers but facilitate the advertising technology that keeps these systems operational.

- One example of this technology is advertisement cookies.
- According to NAI, a cookie is a small text file saved to your browser that enable tracking and personalization.
- The NAI, with the DAA, have recently introduced opt-out mechanism for cookies and non-cookie technology such as browser cache, locally stored objects, and other kinds of statistical identifiers.
- NAI and DAA now offer a beta website that will give users two different opt-outs for a company that uses both cookies and other technology.

Additional Methods of Advertising Tracking and Opt-Out

- In addition to the methods of tracking discussed above there are a few more ways that advertisers can learn more about users.
    - Users may be tracked through mobile technology in their vehicle.
    - Unique device identifiers can track either standard computers or mobile devices.
    - Audio watermarking is used to send audio signals to devices that cannot be heard by users to distribute advertisements.
    - Cross-device technology allows advertisers to learn if one user on a device is the same user on another device.
- If a user opts-out of interest-based advertising, the device which is used to access that system is also opted-out of cross-device tracking.
- The opt-out mechanism still allows companies to create device graphs (which note which devices are tied to the same user) and only applies to interest-based advertising.
- In order for a user to be completely opted-out of interest-based advertising that user must opt-out on all of their devices.

How is Data Used in Targeted Advertising?

- Data can be used to improve and personalize a user's experience.
    - For example, Netflix uses collected data to present users with video content recommendations based on past video content viewing.
    - Increasing, the application of AI and machine learning is used to analyze collected data to improve predications about consumer behavior.
    - Certain formulaic associations between types of behavior and desired audiences may be used for advertisers to help find those desired audiences. Many people at FPF are trying to figure out how that can be done fairly and safely.
    - Data can be used to link devices in order for consumers to feel more comfortable about using a service across multiple devices.

Adam Towvim (Chameleon Collective) on the evolution of ad-tech and the ad-tech value chain

The beginning of ad-tech online

- In the early 1990s ad-tech was very inefficient and consisted of a particular advertiser going through a lot of loops to get advertising to a consumer.

- Advertisements to be posted had to be sent via fax.
- The advertiser had to go to every publisher individually to get advertisements out.
- This process involved multiple publishers with multiple contracts which created difficulties for both advertisers and publishers.

Solutions to the initial ad-tech issues

- A network of publishers (ad-network) evolved to handle single advertisers wanting to reach multiple publishers through contact with a single ad-network.
- The ad-network also created publisher "buckets" where a specific type of advertiser could reach multiple publishers of the same type (i.e. sports, entertainment, etc).
- Though the ad-network model did create more efficiency, advertisers still had very little information regarding how to set advertisement market prices and reach more platforms.
- To solve this problem, highly efficient ad-exchanges were created.
- Ad-exchanges allow advertisers to submit advertisements which are bid on by publishers in an auction.
- With ad-exchanges millions of advertisements can be submitted and bid on within a very short time.
- Geo-data brokers additionally provide advertisers with region specific publishing platforms using geo-fences and other geo-locating functions

Understanding User Data

- Matching data across websites and apps, sometimes with email addresses or unique user IDs, allows more accurate and relevant messaging based on user activities on other websites.
- Matching data also allows advertisers to go to off-line data brokers and learn what a particular user has bought in person (such as at a grocery store or value card).
- Persistent tracking is also aided by unique identifiers that exist on a user's device. The vast majority of devices are from Apple's IOS advertising identifier and Androids Ad-identifier that Google issues.
    - These are unique identifiers that are issued by the operating system that are unique to that device at that point in time and are resettable by a user.
    - Generally, a very low number of users reset their mobile Id, but more users are engaging in the process out of concern for privacy issues.

Maximizing Advertisement Effectiveness

- Once data about a user and that user's behavior in relation to advertisements has been aggregated, advertisers try and understand how effectively the advertisement reached the consumer.
- Advertisers are interested learning if particular advertisements and publishers:
    - Increased overall sales;
    - Increased the number of potential customers willing to sign up for email lists; and
    - Increased the number of online advertisements that lead to offline sales.

- Multiple advertisement-focused function groups work to bring together all of the user information collected to measure whether the individual who is exposed to an advertisement on a website eventually purchases a product.
- Information about the effectiveness of an advertisement (if it led to a sale) is often based on inferences of consumer behavior and not determinative. These probability assumptions have a high degree of likelihood.
- Ultimately, the driver of all this data-focused advertising is to determine if there is a high return on the funds spent on an advertising campaign.

Question & Answer

Question: What exactly can users opt-out from when they opt-out of advertising?

Answer: Users are effectively opting-out of the placement of cookies on their browsers and computers. They are opting out of the tracking of the device ID, but this is one of the things that we really wrestled with when we came up with the DAA guidelines. If you look at the EU model, they make sure that data is wiped clean. From a mobile perspective, opting out is a little cumbersome because not all of the identities between multiple devices are the same. Users need to be aware that they need to opt-out from multiple devices to be truly opted-out. The FTC has been particularly concerned lately about users not understanding that each device must be opted-out, even on mobile. Advertisers may still use user information to improve their website and various other purposes.

Question: Who is bound when a user opts-out?

Answer: Third parties within the advertisement ecosystem who are enabling ads, first parties who would otherwise be sending that data. There is a collaboration amongst different players in the ecosystem that they effectively have to honor that opt out.

Question: How does a website our ad-tracker know when a child is using the website or app with ad-tracking?

Answer: The short answer is that they don't know if a child is using the website or app. We know that in ad-tech there is two things. One, the property—the mobile app, the website—is seen as a child directed property such as a Disney website or app that is targeted to someone younger than 13 years old and under federal law no one can build a consistent profile on someone below the age of 13. Two, the property could be a broader site with a broader audience that does ask for age. If the property asks for age, then it passes the age information along with the advertisement requests and the online advertisement platforms need to be sure they are not targeting users below the age line. Additionally, some sites offer different, child-focused, configurations.

Answer from attendee: Some trackers offer "child" configuration, where it signals to the tracker that they are dealing with a child audience and so treat the data differently. However, primarily, the onus is on you to do the diligence: review the privacy policy, terms of use and business model for your ad providers, analytics companies, etc. Get agreements in place with them to restrict their use of the data when dealing with children - and, of course, to align with the education privacy regulation (FERPA and state laws).

Question: Why do advertisements have to exist?

Answer: Most people do not like to see advertisements. However, if you ask people if they would prefer to see advertisements or paying for website content, what you find is that the number of people who would prefer to pay for the website is very small. The value of advertising is foundational to much of the online and media experiences we have today in the same way that it funded free television for decades. For more justifications go to the IAB (Interactive Advertising Bureau) website. Publishers wrestle with being able to fund their product roadmap and not annoying their users. Typically, this is referred to as a value exchange.

Question: Where's a good source to get some insight on what these terms mean?

Answer: The IAB has a glossary of terms of art that we are using here today and if you just type IAB and glossary into your google search it should come up as the first option. The Network Advertising Initiative also has some information on these terms.

Question: How can folks tell the difference between a tracker used for analytics vs. a tracker that is sent to an ad-tracker?

Answer: I don't think that you can tell from a technical standpoint but the self-regulatory websites require the use of the "Ad-Choice Icon" on an add which should tell you which companies are collecting data related to that add. Also, when you go to the opt-out page of these organizations and they will scan your browser and let you know what tracking is happening on your device.

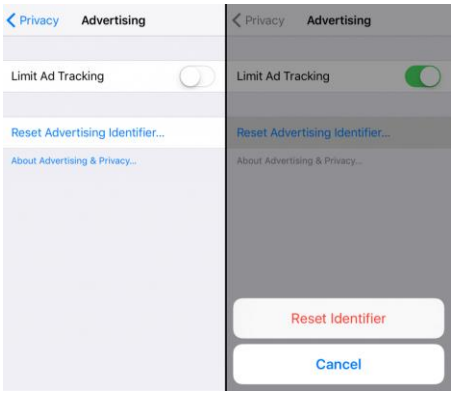
Additional Questions Answered in the Q&A Google Document By Speakers or Attendees

Question: For iOS and Android, can a group policy be created to manage the settings or is it up to each individual? I am asking this in the context of education.

Answer: For iOS, chiming in from the district practitioner side on this, this depends on if this is a personal/BYOD scenario or a district provided shared or 1-1 scenario. If district provided, typically these will be using accounts created under the managed apple ID program (https://support.apple.com/en-us/HT205918) and the device is likely managed via an MDM with Configuration profiles, one of the policies is "forceLimitAdTracking" (https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html).

Question: What are the links to the two sites to opt out?

Answer: http://optout.networkadvertising.org/#!/ and http://optout.aboutads.info/#!/. On mobile, the DAA has an app that allows opting out on a mobile device. An iOS, the "Limit Ad Tracking" tag also zero-s out the mobile advertising identifier (see: https://fpf.org/2016/08/02/ios-10-feature-stronger-limit-ad-tracking/):



Learn more here: http://www.nytimes.com/2015/12/21/business/media/key-to-opting-out-of-personalized-ads-hidden-in-plain-view.html

Question: How can you tell if a website has ad trackers?

Answers:

- Use "Ghostery"/Evidon Browser extension
- TrustArc, Evidon and others offer a service that makes it possible to see if a website has ad trackers

Question: How are hashed identifiers like an email address matched via tokens across such disparate systems? Is there a common standard used to enable a definitive match?

Answer: Usually it's a "SHA1" hash or similar (typically stronger) hashing algorithm. See here for why.

Question Follow-Up: But usually tokens subscribe to a common standard to reinterpret the data thru 1:1 agreement. How does this happen with so many players?

Answer: It's a little informal, in that the largest platforms will typically coalesce around one standard, like MD5, then SHA1, and now SHA256 is seen as even stronger. Also, make sure to search for "salted hash" where, even though a publicly-available (and theoretically non-reversible) standard like SHA1 is used, people will still overlay a Private hashing algorithm, known as a "Salt"