Hashed & Salted | A Privacy and Data Security Update
June 2022

Animal Crackers in Acronym Soup: Understanding Adtech Proposals for a Cookieless Future

Much has been made of the long, slow demise of third-party cookies. Cookies and tracking tools power the digital advertising ecosystem by identifying particular web users and serving them relevant content based on their browsing behaviors. Third-party cookies also serve operational purposes, including ad campaign measurement and attribution. Now, the drumbeat of increased privacy regulation, changes in platform policies and regulatory scrutiny continue to chip away at this feature that underpins the online advertising world.

This changing landscape has pushed the industry to develop alternative proposals and solutions to allow advertisers to continue aiming their ads at receptive audiences. Many companies are considering leveraging one or more of these "cookieless" targeting options, including through relationships with various partners that offer such solutions. Many of these alternatives provide solutions to technical issues while also implicating privacy considerations. In response, industry groups have offered related programs and guidance on best practices for using certain new alternative identifiers. We help break down the bird references in this menagerie of acronyms so that leaders across a variety of functions can speak the same language.

Distributed/Universal ID Systems

Initial proposals in this area focused on finding a new, standardized identifier that could still allow a group of participating organizations to universally identify individual users across different websites and devices. This may sound familiar; the difference lies in how these solutions create this "universal" identifier. Several solutions use hashed email addresses as a cornerstone.

Specifically, these solutions provide a standard for securely transmitting new unique IDs that are based on matching to a common email address. Some universal IDs operate within one environment (e.g., only within web browsers). Other universal IDs are offered along with a device graph, which can help match universal IDs generated across devices (e.g., in a web browser and on a smartphone). Solutions that fall into this category include ID5, Unified ID 2.0, RampID, the Secure Web Addressability Network (SWAN)community, and others.

These solutions are offered as an alternative to syncing different cookie-based identifiers from various tracking tool providers; matching up various cookie IDs can be slow, inefficient, unreliable, resource-intensive and—crucially—a dead end once third-party cookies no longer function. Universal IDs are also offered as an alternative to the "walled garden" approach that focuses on a specific platform's first-party data. That said, these solutions also potentially face certain challenges, since they still identify a particular individual and rely on a specific identifier to do so. In particular, regulators in the U.S. and the EU have expressed some concerns about the use of hashed identifiers. While these are technical solutions that may address certain issues caused by the loss of third-party

Attorney Advertising

cookies, the identifiers themselves may be treated as personal information and their use will be governed by applicable privacy laws.

Cohorts

Solutions in this group rely on federated learning, which we covered previously in "Pivot to PETs: What You Need to Know About Privacy Enhancing Technologies." Machine learning usually relies on taking large amounts of data, centralizing that data in one place and training artificial intelligence (AI) models on that data set. In contrast, federated learning trains AI models in a decentralized way. The training happens within a user's device, using data locally stored and accessed within a browser or on the device. This removes the need to aggregate large sets of data in one place, like the cloud.

These solutions are also focused on shifting away from one-to-one advertising—i.e., one ad targeted to one user. Instead, the goal is to advertise to a group of thousands of similar users, or cohorts, based on similarities in their browsing behaviors. Whether a user belongs to a particular cohort or interest group is recorded by a browser, not centrally within a platform or in the cloud. As a result, the information about interests and interest groups is distributed across browsers. Some solutions would have auctions and bids for ad placements take place locally at the device level. Other proposals would reduce the granularity of audience interests while also routing traffic through a proxy service, anonymizing some data and adding noise to other pieces of data. Solutions that fall into this category include FLEDGE, Topics, and PARAKEET.

These solutions would also function without cookies, but various proposals may need to be combined to re-create the full functionality of third-party cookies. For example, one solution may enable targeting, while another would allow retargeting and a third would help with measurement and attribution. These tools are currently going through testing, and open questions remain as to whether they will be broadly adopted or accommodate additional privacy signals and choices.

Aggregated/Attribution Reporting

Cookies perform more than just marketing and retargeting functions. They also help advertisers track whether a particular web user clicked on an ad, visited the advertiser's site, and then made a purchase. Tracking this user journey requires "attributing" a particular user click to a purchase. Without cookie IDs to follow the user at each step, alternatives are needed to allow browsers across devices to match information and still measure attribution events. Certain platforms provide application programming interface (API) based solutions that allow for attribution in this way, usually based on whether users are logged in on their platforms. Another proposal, called Interoperable Private Attribution (IPA), would use open-source device "match keys" that are also tied to a login.

Browsers that are "interoperable" on one of these standards would be able to match the same user logging into the same browser, or potentially even a separate browser on a different device at a later time. The match key could then connect an ad seen on one device to a purchase made on another device or browser. These attribution systems would send out batched reports that show only the number of conversions that could be connected to a click on an ad, not individual-level conversion data. Modeling is then based on sets of users rather than individuals. These solutions are currently fairly specific to a particular platform, while some functionalities and the level of adoption are uncertain.

Industry Oversight Programs and Guidance

New resources from existing self-regulatory associations aim to help provide guidelines and parameters for new identifiers and advertising technologies. The Partnership for Responsible Addressable Media (PRAM) is a cross-industry initiative made up of advertisers, publishers, agencies, platforms and others and is administered by the Digital Advertising Alliance (DAA). Earlier this year, PRAM and the DAA announced a policy framework to help standardize governance for providing and using interoperable addressable media identifiers (AMIs) in the digital media ecosystem. The framework lays out a certification process for specific AMIs, establishes specific permitted uses, and integrates accountability measures through the DAA's existing Self-Regulatory Principles to help make sure that AMIs are used only for authorized and responsible purposes. The DAA recently announced the launch of its initial certification process for AMIs, with TrustArc serving as the first compliance partner to manage the review and attestation process by AMI

providers. As a start, LiveRamp has committed to undergo AMI certification for its RampID and Authenticated Traffic Solution.

The IAB Tech Lab and its Project Rearc Initiative have launched the Global Privacy Platform (GPP) to consolidate privacy signals sent for digital advertising. The GPP is a "single protocol designed to streamline transmitting privacy, consent and consumer choice signals from sites and apps to adtech providers" across digital media channels, with integrations into existing privacy signals such as Europe's Transparency & Consent Framework and the United States' Privacy User Signal under the California Consumer Privacy Act (CCPA). The IAB Tech Lab and Project Rearc are currently taking public comments on the platform.

Finally, the Network Advertising Initiative (NAI) has issued new Best Practices for User Choice and Transparency, intended to explain consumer choice and transparency obligations under its existing NAI Code. The guidance is also intended to help companies avoid dark patterns and instead maximize effective and efficient notice and choice mechanisms when collecting consumer data. The phrase "dark patterns" generally refers to elements of user experiences or interfaces that deceive users into doing things they don't intend to do, as our recent In The Know video "Shining the Light on Dark Patterns" describes alongside some practical examples.

What questions should you be asking?

It remains to be seen which, if any, of the industry proposals will gain widespread adoption. In the meantime, here are several key questions to ask your teams about digital advertising technologies, proposals and solutions they are considering to navigate a cookieless future:

1. What solutions and technologies do we rely on for digital advertising today?
2. How will they work if third-party cookies no longer function?
3. What problem will a specific new solution, technology or proposal solve?
4. What specific data, if any, will this solution collect and use?
5. Where will the data be stored (on a device, in the cloud, on the premises, with a third party)?
6. Does this solution participate in or commit to any industry guidelines?
7. How will we test and monitor whether this solution is effective?
8. What contractual protections is the provider of this solution offering?

If your teams have not brought one of these solutions to you, consider talking to them about the technical challenges the loss of third-party cookies can present for their future marketing plans. Don't forget to make sure that all parties are using terms like "pseudonymous," "de-identified," "anonymous" and "personal data" consistently and in line with their legal definitions.

These questions can help you vet the various solutions available and determine whether a particular provider's offering will help your teams further their marketing goals while managing privacy implications.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Caroline W. Hudson . . . . . chudson@loeb.com