Survey Of Alternative AdTech Solutions In The Face Of Third Party Cookie Deprecation

Sponsor: ZenData
Advisor: Prof. Hana Habib
Team: David Mberingabo, Pauline Mevs, Sriram Viswanathan

Carnegie Mellon University
MSIT-Privacy Engineering Capstone Project

August 2023

Since the early 2000s, third-party cookies have been repurposed by advertisers and intermediaries to monetize online advertising and sustain an ad-sponsored open internet. As the internet expanded, entities devised numerous methods to gather user data for tracking and targeting. Increased awareness among consumers and regulators about these practices' privacy infringements prompted regulatory action to establish privacy rights and enhance transparency in online advertising. Global regulations, with a focus on third-party cookies, deceptive consent tactics, and online advertising monopolization, led to self-regulation efforts by browsers and the advertising industry. This included third-party cookie deprecation, whereby browsers no longer support these cookies, compelling advertisers and publishers to explore alternative solutions. However, these alternatives vary in privacy enhancements, targeting capabilities, and data fidelity compared to third-party cookies.

With the deprecation of third party cookies, publishers are looking for ways to protect their revenues, which often leads them to finding alternative solutions that enable audience addressability and reporting ad campaign effectiveness. Publishers are considering ways of leveraging first party data, that also protect users' data and comply with regulations. Deprecation is also an opportunity for brands and publishers to build increased trust with their customers and provide richer value exchange for the data collected to the users.

In our study, we looked at the current state of these alternative solutions and what AdTech use-case do they solve (viz., audience addressability, or data sharing and enrichment, or measuring campaign effectiveness). At a high level, these solutions can be classified into alternative ID solutions, Data Clean Room (DCR), Seller Defined Audience (SDA), and Privacy Enhancing Technologies or PETs. In addition to this, Google is introducing its Privacy Sandbox suite of APIs and features that are built into Chrome (the largest browser by market share) to enable a more privacy-preserving way for both interest-based advertising (IBA) and ad attribution reporting. All these solutions have varying degrees of maturity, adoption, ease of implementation, privacy guarantees, and last but not the least, utility to the use-case for which it is being used in terms of measurable ad metrics that can help with the choice of the right solution for the right use-case.

Even though alternatives to replace third party cookies are proliferating, marketers, publishers, and other entities will not commit the funding and prioritize efforts to adopt solutions as long as third party cookies are still in use. This is in part because of missing independent analysis measuring the effectiveness, privacy, and quality of alternative solutions are missing.

Our study also involved discussions with a range of advertising industry stakeholders, including advertisers, developers, tourism companies, AdTech leaders, academics, and legal experts. In our discussions, participants echoed that what they are looking for in a solution is information to categorize (i.e., identify and create audience segments), track (i.e., cross-site tracking), and reach potential customers (i.e., publish on the right site) and obtain and use this information as cheaply as possible. A few participants mentioned needing to be able to share this information with partners for further marketing.

The upcoming regulations, notably the Digital Markets Act (DMA), are raising concerns about the impact of these alternative solutions on privacy and the advertising ecosystem. The effectiveness of DMA remains uncertain, relying on regular oversight and communication with companies rather than legal actions for enforcement, with the European Commission empowered to impose fines up to 10% of a gatekeeper's (i.e. large digital platforms like Google, Apple, Facebook, and Amazon) global revenue for violations. The DMA requires platform participation for interoperability changes, while Google's Privacy Sandbox, a separate move from third-party cookies, faced scrutiny due to existing laws. Notably, major tech firms, including Google, opposed the DMA. With the shift from third-party tracking to first-party data and new solutions in the AdTech landscape, regulatory demands for user consent clarity and data transparency increase under DMA, the ePrivacy Directive (ePD), and GDPR. These rules reject "cookie walls" and emphasize alternative content access methods. The consequences of these shifts on industry practices remain uncertain.

To accomplish precise ad targeting, the ecosystem requires more and more data from the users. Due to the fragmentation of information retained by different parties, stakeholders would like to merge their otherwise siloed datasets and further deduce key attributes and behaviors from a individual's data to build enriched profiles. This need for rich profile building conflicts with the privacy need of the data subjects. To accommodate for consumers' thirst for privacy, publishers will have to evolve with the times and adjust their monetization and business strategies accordingly.

The outlook for these alternative solutions is unclear at the moment, with each having varying levels of adoption, maturity, complexity and regulatory implications. It's anyone's guess which solution will ultimately prevail in the long run. Until then, the landscape is quite scattered, making room for innovation in terms of privacy-preserving technologies, regulations, as well as value to the AdTech participants.