Niklas Ekman
Associate Director,
Data & Analytics

December 13, 2021

The Rising Concern of Digital Privacy & Security

As digital security and privacy becomes an ever-growing concern, from database breaches, to corporate leaks, and social media whistleblowers, the pressure on Big Tech to protect it's users and their data is bigger than ever.

Facebook, for example, has been accused of putting shareholders above their users by focusing their news feed algorithm to serve content tailored to induce strong emotions—often negative ones—since these emotions will by extension generate engagement. It's this ad-driven model, fueled by user data, that is seen as part of the larger narrative of digital privacy and security.

One solution to Big Tech's data problem could be pushing these services behind a paywall, effectively eliminating the need to sell their users' data or have ads drive their business model. A competitor to Google, Neeva.com, offers precisely this: a paid subscription search engine that wishes to eliminate the need to serve ads. But, given Googles almost $2 trillion dollar market cap, it isn't likely that they would shift their entire profit engine or business model anytime soon. However, one thing that Google has decided is to phase out third-party cookies on its Chrome browser starting 2023.

A third-party cookie, as described by Cookie Script:

> Third-party cookies are cookies that are set by a website other than the one you are currently on. For example, you can have a "Like" button on your website which will store a cookie on a visitor's computer, that cookie can later be accessed by Facebook to identify visitors and see which websites they visited.

And with Chrome having a 65% market share, this will have a clear impact on most users as they get more control over what data they want to share and a better understanding of how they're tracked. In addition, the ban should lead to stronger data privacy across internet users and not only for customers of brands asking to track their behavior. But what does this mean for marketers?

How a Post-Cookie World Affects Advertising

From the introduction of email marketing, to paid search, the influencer economy, the explosion of podcasts, and TikTok, advertisers have always tried new technologies. Wherever new knowledge about an audience becomes available, whatever new method is introduced to communicate with said audience, advertisers have eventually been there to try it.

Will Contextual Advertising Eat the Third-Party Cookie?

Usually, this technology has continued to morph, evolve, or expand, but as times change so does the advertising and MarTech landscape. How will advertisers react when pieces in their ever-growing tool kit are suddenly taken from them? Let's start by looking at the impact that removing third-party cookies will have.

Advertisers will have to generate new tactics to identify audiences as customers move across the internet. In addition, organizations selling advertising data will have to identify new methods to collect and compile audience data. Digital publishers who relied on third-party cookies and their associated data will see that revenue disappear. Social media websites that used to track audience behavior on advertisers' websites through cookies – one such example could be a like button – will now have to adjust their targeting strategy.

Advertising solutions once the third-party cookie has crumbled

1. Optimize the Collection of First-Party Data
   It can be argued that there is no data that is more dependable than first-party data. These consumer interactions—people-based, personal, email addresses and other identifiers collected across your various touchpoints including websites, marketing efforts, and apps – will be tremendously valuable when third-party cookies disappear.

2. Build Strong Relationships With Second-Party Data Providers
   Second-party data is the first-party data of another organization. By building strong partnerships with businesses that carry relevant first-party data you may leverage it to optimize audience targeting.

3. Match First-Party Data With a Unified Domain
   If you collect your first-party data properly, you will build a valuable profile of your audience, and once they log in to your website you will be able to track their behavior. However, if your audience must click across multiple domains this could cause friction in the holistic view granted by a single domain.

4. Leverage Contextual Advertising
   Contextual advertising is sometimes considered a targeting method from the old marketing playbook. With contextual targeting a branded ad is placed on a website where the topics mentioned are of contextual relevance. In other words, a website featuring a "Ten-step tutorial on how to ski" could feature an ad to buy skiing equipment. This isn't much different from the typical process of paid search where brands bid to have their text-based ads show up for relevant keywords. Contextual targeting focuses on the context of a website rather than the searches on a search engine.

Contextual targeting offers several benefits

- It's not limited by current data privacy law
- It can provide brand safety
  - Prevent an ad placement from showing up on websites that are irrelevant or in opposition to the intended use case of the ad

Evoke

Will Contextual Advertising Eat the Third-Party Cookie?

- Context can also be more relevant than behavior
  - A small business owner who has a hobby might not want to be targeted by ads for accounting software when they're reading about their favorite TV show or cooking recipes
  - However, sometimes context doesn't indicate desire; an article about flying to Hawaii doesn't necessarily mean that the reader is currently in the market for a hotel in Hawaii
- Contextual targeting allows relevance without being creepy
  - A lot of people find that constantly being retargeted by ads is an unsettling experience, almost as if they're being stalked online
- Contextual targeting is smarter than ever before
  - Today, contextual targeting has started to leverage AI and ML to incorporate natural language processing and computer vision in its placement decision. This advancement has improved relevance in terms of which website should or shouldn't show an ad

Summary

With data privacy concerns on the rise Big Tech is forced to adjust how they handle their users' information. Google has, as an example, responded by removing the third-party cookie from their Chrome browser. As a result, advertisers will have to figure out new methods to target their audience. One solution is to leverage contextual advertising, and while some considered this an outdated method of targeting, others have pushed the technology forward. Today, contextual advertising leverages AI and ML to scan the components of a website more accurately. From text to images and videos, these algorithms continue to get better at understanding when it's relevant to place an ad on a website. For more information, email us at: **business@evokegroup.com**

1. https://www.upguard.com/blog/biggest-data-breaches
2. https://www.theverge.com/2021/10/6/22712250/twitch-hack-leak-data-streamer-revenue-steam-competitor
3. https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress
4. https://qz.com/1039910/how-facebooks-news-feed-algorithm-sells-our-fear-and-outrage-for-profit/
5. https://neeva.com/
6. https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/
7. https://gumgum.com/contextual-insider/contextual-articles/contextual-advertising-101

Evoke