ADNUNTIUS

What does it Take to Be Truly Privacy Safe?

As privacy legislations such as GDPR become stricter, more publishers are finding themselves in need of advertising technologies that help in keeping their properties monetized even when a website visitor does not consent to any kind of tracking.

Not all ad serving technologies were created equal and nor were many ready for the world we currently find ourselves in, a place where no cookies or other tracking mechanisms can be utilized, leaving an increasing portion of publishers' traffic completely unmonetized.

Taking Denmark or France as an example, local legislation forces website owners to ask visitors for permission to collect data, they must also make the option to reject as easy as it is to approve.

But, UX has been a publisher's best friend in these markets and possibly why 70% of users still allow data collection - the "accept button" is colorful, larger, and aligned to a user's point of vision, unlike its smaller, grey looking sibling, the reject button, that is hiding in the bottom righthand corner.

70% opting in is an achievement but if 30% of a publisher's inventory continues to remain unmonetized, it has serious consequences for the overall bottom line.

Like Adnuntius, more technology companies have started to offer "cookieless ad serving" as part of their value proposition – but what does that really mean?

ADNUNTIUS

Below, we share our point of view on what it takes to be truly privacy safe, but it is up to you as a publisher on how far you want to take it! Our goal is to provide you with a set of requirements or guidelines that you may which to consider when choosing a technology partner for privacy safe ad serving.

1st and 3rd party cookies, and local storage.

Starting with your website, let's assume that an ad request will be made by dropping a javascript on the page (most common).

Firstly, ensure that the javascript can be modified to block all cookies and whether it comes from the ad server itself or from a third-party ad server (I will expand below on 3rd party ad servers). Finally check that the technology does not write anything to local storage.

Third party code.

The above script takes care of images, text and videos uploaded directly to your ad server. But much of direct advertising comes from either third-party ad servers (served using third party tags/scripts) or HTML5 creatives. HTML5 and third-party tags allow advertisers to upload scripts and ads from third parties that might use cookies.

It is worth noting that those scripts and ads from third-party systems are not under your ad server's direct control.

Any reputable system will no doubt have the functionality to help you to block cookies from third parties, which, as a general rule, will work well on browsers such as Safari, Firefox and Brave, but on browsers such as Chrome or Edge, some 3rd party cookies will manage to slip through.

A few vendors will claim to be 100% watertight so, if you are in doubt, feel free to reach out to us and we will provide you with some creatives that will put their systems to the test.

If you promise no tracking, then do not allow anyone outside your company to do it either. Ultimately it is your responsibility to ensure that if any self-service features are offered, that you have the option to block any HTML creatives and 3rd party tags from being uploaded and used.

Server-side cookies.

Server-side cookies are known as "sessions". A website stores a single cookie on the browser containing a unique session ID. Status information is stored on the server and the ID is used to match the request with the data stored on the server. And now sessions can store user preferences and more.

For anyone that thinks privacy can live hand in hand with programmatic advertising, we have some bad news for you!

Bottom line - if you do not control the server on which the creative is stored, you do not control your website either - which in simpler terms, means that if you do not control the process of creative uploading and the servers that the creatives were uploaded to, then you cannot guarantee that your site does not track the users either.

And since programmatic advertising is based on the ability for buyers to use their DSPs whilst you rely on SSPs, programmatic advertising is really like a box of chocolates “you never know what you're gonna get!”

Some have argued that this is taking it too far. But website owners, or controllers to use a GDPR term, are responsible even in the event of a cyber attack, so it is worth mentioning that known and common methods should at least be considered blocked before you give your website the privacy thumbs up.

So, what can you do?

Yes, there are limitations to what you can do in the absence of user tracking, but we feel that the future is far from bleak and like to think that the industry is entering a renaissance period – a return to well executed creative that is environmentally aligned with content, whether that is the vertical web or by using contextual targeting.

Obviously neither of these options are anything new, but both are effective and proven targeting methodologies for brands wanting to engage with users.

Contextual targeting is understandably a very hot topic of late so by ensuring that your provider can still offer alternative targeting methods without the use of cookies will aide in future proofing your business.