>THE IMPACT OF COOKIE SYNCING ON DATA LEAKAGE AND ENERGY CONSUMPTION<

>OVERVIEW<

The advertising world as we know it is changing. Third-party cookies are on their way out but are still available and very much used in Chrome. The process of cookie syncing presents significant consequences for publishers. **ID5 has commissioned a study to Sincera to assess the damaging implications of cookie syncing by looking at 63,604 domains.**

>WHO INITIATES COOKIE SYNCING CALLS?<

Publisher Initiated Identifiers: Solutions that the publisher has explicitly configured and deployed – often with a contract / legal agreement.

Third-party Initiated Identifiers: Identifiers that are called and written by entities, with limited to no publisher oversight, configuration, or agreement - also referred to as “piggybacking”

>COOKIE SYNCING EXPOSES PUBLISHERS TO DATA LEAKAGE<

The cookie syncing process enables ad tech partners to synchronize their cookies which allows them to communicate a user’s identity through the digital supply chain. The process happens on publisher websites to make their traffic addressable to the buy-side. However, **cookie syncing doesn’t always happen with publishers’ knowledge or approval.** It is common for a publisher’s partners to synchronize with other third party vendors that the publisher has no direct relationship with.

>PIGGYBACKING<

Piggybacking happens when an adtech company drops a third-party cookie on a publisher's website without the publisher's authorization or knowledge. They do this by obtaining access from another ad tech company that received authorization from the publisher.

This **exposes publisher data to unauthorized third parties.** Besides causing compliance risks, it also enables piggybacking platforms to build user profiles, allowing them to reach that audience elsewhere without buying any media from the original publisher.

>THE SCALE OF THE ISSUE<

5.25

is the average number of identifiers that publishers knowingly configure and deploy

14.84

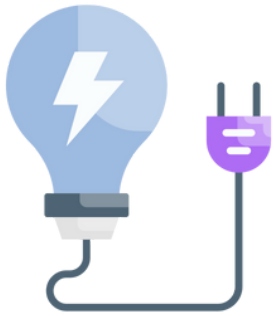
is the average number of cookies written directly by publisher approved partners

1.27

is the average number of audience providers publishers knowingly configure and deploy

62.44

is the average number of cookies set on an ad-supported publisher that the publisher hasn't directly approved or configured



>COOKIE SYNCING IS A WASTE OF ENERGY<

Cookie syncing is an unnecessarily energy-intensive process. The industry is finally becoming more and more aware of the impact that our operations have on the environment. With the drive towards net zero, **publishers and ad tech players must consider how to reduce their carbon emissions**, with cookie syncing being a key area to address.

22.57%

of network traffic is known user sync domains for adtech companies

37.43%

is what this number increases to if you only include publishers with at least one user sync event

23.3%

of publishers have user syncing as more than **50%** of their total network traffic

>SOLUTIONS TO THE PROBLEM<

A high percentage of cookies on a publisher site is not configured or deployed by the publisher and a significant amount of unnecessary network traffic is used for cookie syncing. **Cookie matching is incredibly inefficient and creates regulatory risks for publishers, privacy concerns for users, and a negative environmental impact.**

Thankfully, **there are solutions such as universal identifiers that can solve all of the issues above** and make the identification process much more efficient and profitable for publishers. Standardizing the industry on a handful of identifiers will not only overcome the addressability loss associated with each cookie sync in the chain but also positively impact page load time and user experience as well as reducing overall environmental impact. **The good news is that their adoption is increasing.**

>SHORT AND LONG-TERM FIXES<

Migrating the entire industry to universal identifiers is neither easy nor quick. In the short term **publishers can take the following actions to combat piggybacking and energy waste:**

1. Ensure your cookie syncing is only conducted when the **user has granted consent** to specific vendors
2. Future-proof your business by **selecting consent-based universal identifiers** that have data protection mechanisms and ensuring that your SSPs are using it/them
3. **Review Prebid/Wrapper solution settings** to assess who can drop/fire user sync events
4. **Speak to your SSP and DMP to understand who they cookie sync with** on your inventory and what value those third parties bring to you. If they don't bring any, request that they are removed