

Requiem for a Cookie Part 2: The AdTech Phoenix is Reborn

As the world turns anew in 2022, a seismic shift is underway in the AdTech industry as detailed in [the first part of this Requiem for a Cookie series](#): online tracking technology as we know it is likely undergoing a permanent change. More specifically, the third-party cookie, which has been the dominant method for tracking online user behavior, is quickly being phased out—and in many instances pushed out by regulators. Out of the ashes of soon-to-be outdated tracking techniques, however, arise multiple privacy-forward alternatives. Which technique or techniques will ultimately replace third-party cookies, however, is unclear, and 2022 is expected to bring clarity to the plethora of alternative options currently vying for dominance. Pushing for third-party cookie eradication and leading the charge into new alternatives, Europe is a key incubator for new development in the space. Most notably, the [Belgian Data Protection Authority](#) (BE DPA) is spearheading a reanalysis of the Transparency and Consent Framework (TCF) implemented by the Interactive Advertising Bureau (IAB). Broadly adopted within the AdTech industry, the TCF stands today as the dominant consent solution utilized to satisfy EU members' affirmative consent requirements. But the days of TCF's prevalence appear to be waning as the BE DPA is expected to imminently release a decision confirming alleged infringements by the IAB arising from use of the TCF—specifically violations of the General Data Protection Regulation (GDPR) consent and transparency principals. As of the date of this article, the BE DPA is awaiting potential feedback from other European data protection authorities on its draft decision regarding GDPR infringements, and it is expected that this will be one of the first major privacy developments in the AdTech space of 2022. Given the uncertainties around TCF, many AdTech players have been implementing new techniques that are expected to eventually replace third-party tracking cookies. The French data protection authority *Commission Nationale de l'Informatique et des Libertés* (CNIL) already [released a statement](#) warning individual consumers and data subjects that "the end of the use of third-party cookies does not mean the end of tracking Internet users online." [1] To make sense of the array of alternatives that are in development, the CNIL categorized prominent alternative technologies into four categories, as described below:

- **First-party cookies and fingerprinting.** While the eventual deprecation of third-party cookies is anticipated, the vitality of first-party cookies appears strong. Often necessary for certain operations and for website functionality, first-party cookies are only created and stored on the website a user directly visits. The CNIL cautions, however, that first-party cookies can still be exploited by third parties, as they can be configured to "return data via URL calls on the advertiser's domain." [2] A similar tool is known as "fingerprinting" and is another tracking technique whereby the information provided by a user's browser regarding the technical specifications of a user's hardware (e.g., the operating system or screen size) is collected and used to build a user profile. This information, when sufficiently specific, can be used to track users in a manner similar to cookies.
- **Single Sign-On (SSO).** Primarily used to facilitate a user's online connection, SSO allows the user's account to follow the user while browsing other related websites to which the user's credentials apply. The account can then be used as a tracker across those websites.
- **Unique Identifiers.** By tracking users via hashed data relating to a unique identifier (for example, Apple's Identifier for Advertisers or IDFA), third parties can use the login information and email addresses to link usage of various services.
- **Cohort-based Advertising Targeting.** Primarily pioneered by Google's Federated Learning of Cohorts (FLoC), cohort-based targeting avoids targeting individuals by instead clustering a large group of people with similar interests and assigning the group a unique identifier. This enables individuals to effectively

"hide in the crowd" while allowing advertisers to reach appropriate audiences.

In addition to the above methods identified by the CNIL, several other creative tracking solutions are gaining traction within the AdTech industry and are expected to make gains in 2022. First, on one end of the cohort-based spectrum is **micro-grouping**, where small groups of users (between three and five users) are tracked as a single entity in real time. **Zero-party data**, where users intentionally elect to share their preferences and intentions (e.g., a user answering a survey administered by the website host), is data that comes straight from the source, and is regaining popularity in marketing. **Conversion measurement** is getting an overall facelift, but perhaps most specifically through Google's Privacy Sandbox, where notably, Google announced that it is seeking to use "privacy-preserving techniques like aggregating information, adding noise, and limiting the amount of data that gets sent from the device." [3] Harkening back to more traditional techniques used for generations within the print advertising industry, **contextual targeting** relies on the content of the website a user is visiting instead of user data gleaned from third-party cookies; for example, a website concerning parks and recreation may feature advertising for hiking gear or outdoor clothing to all website visitors, not specific, targeted individuals. The above methods appear to be gaining traction in the AdTech industry, and 2022 is expected to not only bring further developments in these techniques, but also to spotlight clear "winners" in the bake-off to replace third-party cookies. Regardless of which technique or techniques the AdTech industry eventually chooses as the replacement for third-party cookies, it will be imperative that these techniques are designed and implemented with privacy compliance in mind. Along these lines, the CNIL propagated a firm reminder that under existing European privacy laws, *any* action that creates an individual or group profile and involves targeted advertising will require prior consent of the user—even if no personal data is processed. [4] Users must be able to "choose freely and in an informed manner" to refuse such tracking, and indeed, public demand for user choice is expected to continue, as recent years have indicated user focus on privacy transparency and choice. Ultimately, 2022 could prove to be a watershed year in the AdTech industry and may signify the final crumble of third-party cookies. [1] Alternatives to third-party cookies: what consequences regarding consent? (Nov. 23, 2021), <https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent>. [2] *Id.* [3] Building a privacy-first future for web advertising (Jan. 25, 2021), <https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>. [4] *See* Alternatives to third-party cookies, *supra* at [1] (citing the ePrivacy Directive and Art. 82 of the French Act on Information Technology, Data Files and Civil Liberties).

Authors



[Peter Hegel](#)

Counsel

PHegel@perkinscoie.com [312.324.8683](tel:312.324.8683)

Explore more in

[Privacy & Security](#)

Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's [Privacy & Security practice](#), recognized by Chambers as a leading firm in the field.

[View the blog](#)