THOMSON REUTERS
PRACTICAL LAW™

The Post-Cookie Digital Advertising Landscape: Planning for Privacy Compliance in Unsettled Terrain

by Fernando Bohorquez, Jr., Gerald Ferguson, Priyanka Surapaneni, and Yadilsa Diaz, Baker Hostetler, with Practical Law Data Privacy & Cybersecurity

Status: **Published on 16 May 2023** | Jurisdiction: **European Union, United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-038-4579**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

An Article examining digital advertisers' and tech companies' shift away from using third party cookies to track and target consumer behavior across websites, apps, and other online platforms due to increased global privacy regulation and consumer concern. This Article discusses the digital advertising regulatory landscape including the EU ePrivacy Directive, GDPR, CCPA, and other US state consumer privacy laws, emerging alternatives to third-party cookies, and best practices for businesses to develop a privacy-focused, post-cookie digital advertising strategy.

Digital advertising exists in a complex ecosystem that the average person engages with daily. It encompasses a broad set of technologies for managing advertisements across channels including search, display, video, mobile, and social, with functions for targeting, design, bid management, analytics, optimization, and automation. Digital advertising also incorporates many digital tools and systems that target specific individuals and audiences.

The digital marketing ecosystem traditionally centered on tracking and targeting consumers across websites, apps, and other online platforms. Marketers employed third-party cookies (small digital files that websites download to a user's device) to identify and track users across the Internet. Over the last two decades, the third-party cookie remained constant and served as the foundation of the digital advertising system. However, developments in data privacy laws and advertising technology standards have the third-party cookie on track to phase out by the end of 2024, along with the entire behavioral advertising model that it supports.

With this in mind, advertisers and website publishers should begin positioning themselves for the inevitable "cookie-less" world. Against this backdrop, this Article:

- Provides a primer on the cookie and third-party cookies as data tools.
- Discusses the technological deprecation of the third-party cookie.
- Reviews the privacy laws that regulate behavioral advertising.
- Summarizes the emerging alternatives for third-party cookies.
- Provides key takeaways and best practices to help businesses prepare for the industry transition from a consumer tracking framework to a consumer-centric, privacy-forward one.

The Cookie as a Data Tool

Cookies are small text files that a user's browser stores on their computer or mobile device when they visit a website. Websites use cookies for many purposes, including to:

- Identify users.
- Remember a user's language preferences and passwords.
- Simplify or personalize a user's web experience by allowing servers to track user activity on a website.
- Preserve user information while they browse from one page to the next.
- Enable a third party to present online behavioral or interest-based advertising to the user on a different website.

Cookies are classified in many ways, but three key attributes influence their regulation and legal treatment:

- **Lifespan.** These cookies are classified based on their temporal use and include:
  - **session or temporary cookies**, which are only active while the browser is open and disappear when the user closes the browser; or
  - **persistent cookies**, which remain on the user's device for a defined period and remember information like settings, preferences, and login information.
- **Purpose.** These cookies are classified by use case and include:
  - **strictly necessary or essential cookies**, which provide basic functions that enable a website to work as intended;
  - **performance or static cookies**, which include analytics cookies and collect information on how a user navigates a website through pages visited and clicks, usually in an anonymous manner;
  - **functional or preference cookies**, which allow websites to track and remember a user's past preferences and choices on a particular website such as username, password, region, and language to personalize the experience; or
  - **targeting or tracking cookies**, which manage the performance and display of advertisements and help build user profiles.
- **Domain.** These cookies differ based on which host or hosts can receive information from the cookie and include:
  - **first-party cookies**, which send information to the specific website a user intentionally visits, allowing that website to collect analytics data that, among other things, provide a deeper understanding of user habits and personalize the user experience only on that website; or
  - **third-party cookies**, which send information to websites or online platforms the user did **not** intentionally visit, enabling advertisers and AdTech companies to track users' online behavior across websites and deliver personalized or targeted ads (see Third-Party Cookies).

Third-Party Cookies

Third-party cookies enable advertisers and AdTech companies to track users' online behavior and provide them with personalized or targeted ads. These cookies:

- Collect data ranging from a user's geographic location to their browsing or purchase history.
- Can follow a user across multiple websites or platforms.
- Are leveraged by advertisers in digital advertising campaigns.
- Enable numerous key programmatic advertising tools, such as software and algorithms that automate the instantaneous sale of ads and fuel real-time bidding.
- Form the foundation for behavioral advertising as it is today.

Use cases for third-party cookie digital advertising fall into the following groups:

- **Identification.** Supply-side and demand-side AdTech platforms frequently use third-party cookies to identify users across the web. Advertisers then use the cookies for behavioral targeting and retargeting to serve users personalized ads based on their behavior and interests.
- **Frequency capping.** Advertisers use third-party cookies to identify whether a user has seen a given ad a specific number of times so they can limit the number of times they show the user the same ad.
- **Measuring performance and attribution.** Third-party cookies can also help advertisers measure a campaign's performance and run attribution, which allows them to understand:
  - the action responsible for the conversion; and
  - which ads the user clicked, viewed, and led to the purchase.
- **Audience activation.** This function enables advertisers to use data management platforms (DMPs) to create and target audiences across different websites.
- **Cookie syncing or matching.** This use case underlies many of the above examples, as it involves matching cookies from different players in the digital advertising ecosystem into one cookie ID to theoretically identify the same user. These players may include, for example, demand-side platforms, supply-side platforms, and DMPs. However, cookie syncing has limitations and does not always provide perfect matches.

Third-party cookies provide significant value and utility to behavioral advertising. Advertisers may lose extensive scale and functionality when they can no longer rely on third-party cookies to power their digital strategies.

For more information on cookies and other tracking technologies, see Practice Note, Tracking Technologies: Privacy and Data Security Issues.

The Deprecation of the Third-Party Cookie

Many consumers, consumer rights organizations, and government regulators view advertisers' practice of online tracking and consumer targeting over the past two decades as a pervasive invasion of privacy. This consensus has spurred the passage of privacy laws such as the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, CCPA) that regulate, among other things, the use of third-party cookies (Cal. Civ. Code §§ 1798.100 to 1798.199.100; see Global Privacy Law and Regulation). However, the current "big tech" industry cookie phase-out is just as integral to the decline of the third-party cookie.

As early as 2017, Apple and Mozilla announced that their Safari and Firefox browsers, respectively, would no longer enable third-party cookies. However, a large shift occurred in 2020 when Google announced that its Chrome browser, which accounts for over 60% of global market share, would no longer support third-party cookies by the end of 2022. Google has since postponed this phase-out until late 2024 as it workshops feasible alternatives through its Privacy Sandbox initiatives (see Emerging Alternatives to Third-Party Cookies).

Currently, Google's Chrome browser enables first- and third-party cookies by default, although users can delete or block them. Apple blocks first- and third-party cookies on Safari by default, which has already forced website publishers to grapple with a sizable gap in their addressable audience. Mozilla Firefox now provides users with options to block third-party cookies (standard setting), block first and third-party cookies (strict setting), and fine tune their privacy settings (custom setting).

In early 2022, Apple began requiring apps running on its devices to obtain opt-in consent before tracking user activity on third-party apps and websites. It also removed third-party cookies from its Safari browser and launched a privacy feature with iOS 14.5 called App Tracking Transparency (ATT Framework), which:

- Presents users opening an app with a pop-up box that asks them whether they permit the app to track them across other companies' apps and websites.
- Gives users the choice between two options:
  - **Ask App not to Track**, which sends a signal informing the app that the user has requested not to be tracked. The app developer will lose access to Apple's identifier for advertisers (IDFA), which it uses to track user activity across apps other than its own.
  - **Allow**, which permits an app to track user activity across other companies' apps and websites for advertising or sharing with data brokers.

(Apple: If an app asks to track your activity and Privacy.)

Apple released iOS 16 in late 2022. This enabled tools like Safety Check, which quickly resets a user's data and location permissions, and Manage Sharing & Access, which allows users to see an overview of the information they share. (Apple: About iOS 16 Updates.)

Consumer awareness and backlash to third-party tracking have also contributed to a more privacy-conscious web. Internet users worldwide are using ad blocking software, supporting increased privacy regulation, and expressing concern over whether their personal information is adequately protected online. For example, more consumers are using the Global Privacy Control (GPC) browser setting to send privacy signals to websites indicating their personal data consent preferences (see Global Privacy Control: Take control of your privacy). As discussed below, regulators have taken notice and, in some jurisdictions, require companies to recognize GPC signals (see US State Privacy Laws).

Global Privacy Law and Regulation

The proliferation of European and US state privacy laws and regulations over the last several years has directly impacted business' ability to collect and use personal data, including leveraging third-party cookies for digital advertising. This now robust regulatory environment is one of the main drivers behind the third-party cookie phase-out.

The ePrivacy Directive and the GDPR

The EU regulation of cookies dates back almost 15 years. The ePrivacy Directive (Directive 2002/58/EC), which originally focused on the confidentiality of electronic communications over public networks, was amended in 2009 to clearly:

- Apply to third-party cookies.
- Require informed consent for all third-party cookies unless their use was strictly necessary to provide explicitly requested services.

(Article 5(3), ePrivacy Directive.)

Separately, the GDPR took effect in May 2018 and is the main privacy law in the EU. The GDPR requires entities to establish a legal basis to process personal data, such as the data subject's consent. Both the law and enforcement actions make clear that most cookie uses, by their nature, involve processing personal data and cookies are generally considered personal data whenever they can be used to identify users (Article 6 and Recital 30, GDPR). As a result, the GDPR also requires most (if not all) controllers of third-party cookies to obtain the user's informed consent before using them.

The ePrivacy Directive adopts the GDPR's consent definition which requires a freely given, specific, informed, and unambiguous indication of the data subject's wishes, where a statement or a clear affirmative action signifies agreement (Article 4(10), GDPR). For more information on the ePrivacy Directive and obtaining valid user consent under the GDPR, see Practice Notes, EU E-Privacy Directive: Cookie Use and Online Tracking Compliance for Websites Based Outside the EU and Consent Under the GDPR.

Since the GDPR's implementation, EU regulators have generally required that website publishers obtain informed, unambiguous consent through a user opt-in before deploying non-essential cookies on user's browser. Some EU regulators have gone even further. For example, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), France's data protection authority, issued sanctions totaling approximately EUR210 million to Google and Meta for failing to comply with its cookie guidelines and recommendations, which state that website users must be able to reject cookies as easily as they can accept them (CNIL: Cookies: the CNIL fines Google a total of 150 million euros and Facebook 60 million euros for non-compliance with French legislation).

To comply with the GDPR, the ePrivacy Directive, and regulator guidance and decisions, advertisers must generally:

- For each cookie, disclose accurate information in clear and plain language about the cookie's purpose, including the data it collects or tracks, before obtaining user consent.
- Obtain opt-in consent from the user before placing cookies on the user's device (except for strictly necessary cookies). Do not rely on a website visitor's inaction or continued website use to imply consent or condition the provision of services or content on a website visitor's consent to use cookies.
- Provide users with an easy way to reject non-essential cookies.
- Allow user access to website content even if they do not consent to non-essential cookies.
- Document and retain user consent records.
- Provide users with an easy and effective method to withdraw consent.
- Periodically confirm the website visitor's continued consent.

Notably, these obligations apply to first-party cookies as well as third-party cookies. (Article 5(3), ePrivacy Directive; see Practice Note, EU E-Privacy Directive: Cookie Use and Online Tracking Compliance for Websites Based Outside the EU.)

The ePrivacy Regulation

The ePrivacy Regulation will eventually repeal and replace the ePrivacy Directive and aims to:

- Ensure consistency between the ePrivacy rules and the GDPR.
- Ensure consistency among EU Member States.
- Update the scope of the ePrivacy Directive based on new technological developments.

(European Commission: Proposal for an ePrivacy Regulation and Proposal for a Regulation on Privacy and Electronic Communications.)

Like the ePrivacy Directive, the ePrivacy Regulation seeks to impose certain requirements on entities processing personal data in the digital economy. Notably, the current draft proposes that businesses periodically remind users of their right to withdraw consent for cookies, unless a user chooses not to receive such reminders.

The Council of the EU (Council) also makes clear that businesses may make access to a website conditional on cookie consent if the user can choose between that offer and a reasonably priced paid cookie-free version of the site. Moreover, where technically feasible, businesses should permit users to consent to certain types of cookies by adding providers to an exclusion list in their browser settings. (Section 20aaaa, Council Mandate for Negotiations with European Parliament, No. 6087/21.)

The European Parliament, the European Commission, and the Council are currently conducting trialogue discussions on the ePrivacy Regulation. Although this is the final stage in the EU legislative process, it has been a multi-year exercise with no clear end date, and a long implementation period is likely ahead. For more information on the status of the ePrivacy Regulation, see Legislation Tracker, Digital Single Market Strategy: Regulation on Privacy and Electronic Communications (ePrivacy Regulation).

Self-Regulatory Frameworks

The EU's GDPR and ePrivacy Directive requirements have led to the adoption of industry self-regulatory tools like the Interactive Advertising Bureau Europe (IAB Europe) Transparency and Consent Framework (TCF). The TCF is a cross-industry approach to standardizing:

- Compliance with the GDPR and ePrivacy Directive's requirements.
- How website publishers, advertisers, and AdTech vendors:
  - disclose the purposes for which they collect and use personal data; and
  - obtain user consent.

However, regulators are also scrutinizing these self-regulatory tools. In early 2022, the Belgian data protection authority (DPA) fined IAB Europe EUR250,000 after finding that the TCF did not comply with several GDPR provisions, including those concerning the principles of lawfulness, transparency, accountability, and security. The Belgian DPA permitted IAB Europe to submit an action plan for implementing certain corrective measures, which it approved in January 2023. IAB Europe has six months to implement the plan, the details of which remain undisclosed. (Belgian DPA: The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR.)

Meanwhile, the questions of whether IAB Europe is a controller under the GDPR and whether the TCF data strings and signals constitute personal information are pending before the EU Court of Justice (Belgian Data Protection Authority: IAB Europe case: The Market Court refers preliminary questions to the Court of Justice of the EU).

US State Privacy Laws

Some US state consumer privacy laws' treatment of behavioral and targeted advertising directly impacts the use of third-party cookies since they are essential in tracking and profiling consumers. These laws typically grant consumers a right to opt out of personal information sales, targeted adverting use, including sharing for cross-context behavioral advertising, and certain profiling actives, which effectively restricts the advertising ecosystem's ability to track consumers and collect data to target digital advertisements based on their browsing history.

California Consumer Privacy Act and California Privacy Rights Act

California continues to lead US states in consumer privacy regulation. The CCPA imposes various data protection duties on certain entities conducting business in California, and grants California consumers certain rights regarding their personal data. For example, it requires covered businesses that sell personal information or share it for cross-context behavioral advertising to:

- Disclose these practices to consumers.
- Provide consumers with the right to opt-out of the personal information sales or sharing through a Do Not Sell or Share My Personal Information link.

(Cal. Civ. Code § 1798.120(a); Cal. Code Regs. tit. 11, § 7026; see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Personal Information Sales and Personal Information Sharing.)

The CCPA defines:

- Personal information to include a unique identifier, which includes but is not limited to cookies (Cal. Civ. Code § 1798.140(k), (aj)).
- Cross-context behavioral advertising as targeting ads to a consumer based on personal information obtained from their activity across businesses, distinctly branded websites, applications, or services other than the one the consumer intentionally interacts with (Cal. Civ. Code § 1798.140(k)).
- Sharing as disclosing consumers' personal information to third parties for cross-context behavioral advertising, including transactions where no money or any other type of valuable consideration is exchanged (Cal. Civ. Code § 1798.140(ah)).

The CCPA Regulations also require businesses that sell or share consumers' personal information to honor GPC signals, which the CCPA calls opt-out preference signals. Covered businesses must honor the opt-out preference signals for the specific browser or device and any affiliated consumer profile, including pseudonymous profiles. This expands the scope of when a user is "known" to a business to include instances where businesses use probabilistic identifiers to link anonymous users to a certain browser or device. (Cal. Code Regs. tit. 11, § 7025; see CPRA Regulation Tracker and Probabilistic Identifiers.)

The California Attorney General's (AG) recent settlement with Sephora Inc. for CCPA violations underscores business' obligations to notify consumers if they sell or share consumer personal information and adequately process opt-out requests, including GPC signals. The settlement required Sephora to pay $1.2 million in penalties, clarify in its online disclosures and privacy policy that it sells personal information, and provide a mechanism for consumers to opt out of personal information sales, including via GPC. (See Legal Update, California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations.)

For more information on the CCPA, see California Privacy Toolkit (CCPA and CPRA).

Other States' Comprehensive Consumer Privacy Laws

Seven states in addition to California have passed comprehensive consumer privacy laws, including:

- The Colorado Privacy Act, effective July 1, 2023 (Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-1313; see Practice Note, Colorado Privacy Act (CPA) Quick Facts: Overview).
- The Connecticut Data Privacy and Online Monitoring Act, effective July 1, 2023 (Conn. Gen. Stat. Ann. §§ 42-515 to 42-525; see Practice Note, Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) Quick Facts: Overview).
- The Indiana Consumer Data Protection Act, effective January 1, 2026 (see Legal Update, Indiana Enacts Consumer Data Protection Law).
- The Iowa Consumer Data Protection Act, effective January 1, 2025 (see Practice Note, Iowa Consumer Data Protection Act (ICDPA) Quick Facts: Overview).
- The Tennessee Information Protection Act, effective July 1, 2025 (see Legal Update, Tennessee Enacts Tennessee Information Protection Act).
- The Utah Consumer Privacy Act, effective December 31, 2023 (Utah Code §§ 13-61-101 to 13-61-404; see Practice Note, Utah Consumer Privacy Act (UCPA) Quick Facts: Overview).
- The Virginia Consumer Data Protection Act, effective January 1, 2023 (Va. Code Ann. §§ 59.1-575 to 59.1-584; see Practice Note, Virginia Consumer Data Protection Act (VCDPA) Quick Facts: Overview).

These laws indirectly regulate the use of third-party cookies by allowing consumers to opt out of targeted advertising and personal information sales. They generally define targeted advertising as displaying advertisements to a consumer based on personal data the business obtained or inferred across nonaffiliated websites or applications to predict the consumer's preferences or interests. Businesses covered by these laws must stop using third-party cookies for targeted advertising purposes once a consumer residing in those states submits an opt-out request.

Whether a sales opt-out request requires a business to stop third-party cookies from transmitting that consumer's personal information depends on how the parties structured their business relationship and which state the consumer resides in. Colorado and Connecticut's consumer privacy laws align with California and define a sale as the exchange of personal data by a controller to a third party for monetary or other valuable consideration (Colo. Rev. Stat. Ann. § 6-1-1303(23); Conn. Gen. Stat. Ann. § 42-515(26)).

Non-monetary consideration, such as mutual personal information exchanges or enhanced consumer profiles would make the third-party personal information transfer a sale in those states. On the other hand, Indiana, Iowa, Tennessee, Utah, and Virginia's laws all require monetary consideration for third-party personal data transfers to qualify as a sale (Iowa Code Ann. § 715D.1(25); Utah Code § 13-61-101(31); Va. Code Ann. § 59.1-575). Using a third-party cookie to only trade a consumer's personal data for the third-party's services would likely not qualify as a sale when the parties do not exchange any monetary consideration.

To compare the different consumer rights that state consumer privacy laws grant, see Quick Compare Chart, State Consumer Privacy Laws – Consumer Rights.

Compliance with Multiple State Laws

Businesses may find it challenging to coordinate compliance with multiple state laws' requirements. The Interactive Advertising Bureau (IAB) has released a Multi-State Privacy Agreement (MSPA) that provides an updated contractual framework to the IAB's prior CCPA-compliant Limited Service Provider Agreement to help advertisers, website publishers, and vendors with privacy compliance across the five new state laws. The MSPA employs a set of specifications for privacy strings that maintain consumers' preferences for all five jurisdictions. Businesses can use these with the IAB's Tech Labs US State Signals initiative, which is part of the Global Privacy Platform (GPP). The GPP is a protocol designed to streamline the transmission of privacy, consent, and consumer signals from websites and apps to AdTech providers and will support US state-specific privacy strings for all five states. (IAB: Multi-State Privacy Agreement and IAB Tech Lab Come Together to Help Companies Comply With New Privacy Laws and Place Consumer Privacy at the Forefront.)

Consent Management Platforms (CMPs) are another critical tool in cookie consent compliance. CMPs provide website publishers and operators with the ability to:

- Meet privacy regulatory requirements, including those in the ePrivacy Directive, GDPR, and U.S. state privacy laws.
- Present users with customized cookie choices and a preference mechanism.
- Automate the consent management process.

Emerging Alternatives to Third-Party Cookies

Onerous privacy laws, increased regulatory enforcement, and widespread consumer concern have left the digital advertising industry searching for third-party cookie alternatives. Since no obvious, ubiquitous solution is available, industry players should evaluate a combination of emerging alternative technologies and their privacy features, including:

- Google's Topics API (see Google's Topics API).
- Google's Protected Audience API (see Google's Protected Audience API).
- Apple's SKAd Network (see Apple's SKAd Network).
- First-Party Data (see First-Party Data).
- Alternative Identifiers (see Alternative Identifiers).
- Contextual Advertising (see Contextual Advertising).

Google's Topics API

Although still in development, Google is planning to replace cookies with standards and APIs that certain tools and technologies set within its Privacy Sandbox. Advertisers will use each API to receive aggregated data on issues like conversion (how well their ads performed) and attribution (which entity is credited for a purchase). Google's Privacy Sandbox represents an alternative pathway for the ad industry, relying on anonymized signals that are not cookies within a consumer's Chrome browser. (Google: The Privacy Sandbox).

After some initial work on a third-party cookie replacement called the Federated Learning of Cohorts (FLoC), Google announced in early 2022 that it was moving away from FLoC in favor of a new Privacy Sandbox initiative called Topics API (Topics). Topics groups users into cohorts or categories by topic, purportedly relieving user fingerprinting concerns through detailed tracking and cohort identifiers. Google also claims Topics will avoid assigning sensitive categories to users, such as race or gender, but states that websites can correlate certain topics to sensitive information. (Google: Federated Learning of Cohorts (FLoC) and Topics.)

Details are still emerging on how Topics works and its impact on advertisers. Google has shared that Topics analyzes a user's local browser history on Topics-enabled sites and assigns certain interests to a user as they move around the web, such as Fitness, Travel & Transportation, and Books & Literature. Currently, the Topics taxonomy includes approximately 350 topics, but Google has stated its eventual goal to increase this number and later outsource the taxonomy to an external party. (Google: Get to know the new Topics API for Privacy Sandbox.) As a reference point, the IAB Audience Taxonomy contains approximately 1,500 audience segments (IAB Tech Lab: Audience Taxonomy).

The Topics API will record the topics of websites each user visits. Each week, Topics will gather a user's five most popular topics plus a sixth random topic on their device. Topics then shares these six topics with the websites that the user visits and the website can then personalize the ads it serves the user. Topics deletes and replaces users' previously gathered topics with updated topics every three weeks. (Google: Get to know the new Topics API for Privacy Sandbox.)

The World Wide Web Consortium (W3C), an international organization that sets and promotes web-based standards, has recently raised concerns about Topics' continued surveillance of a user's online browsing after Google requested an early design review in March 2022. A representative of W3C's Technical Architecture Group expressed these findings on Github, stating that the proposed Privacy Sandbox tool "appears to maintain the status quo of inappropriate surveillance on the web... [and] could...be used to customize content in a discriminatory manner, using stereotypes, inferences, or assumptions based on the topics revealed...." (Github: Early design review for the Topics API.)

Meanwhile, the UK's Information Commission Office (ICO), which is involved in an antitrust investigation of Google's Privacy Sandbox, has declined to comment on Topics' potential pitfalls. There has been no discussion from US regulators on Topics, but it is clear that it is already on the UK regulators' radar, which may signal that the EU regulators will also scrutinize it. (Tech Crunch: UK privacy watchdog silent as Google flicks off critique that its Topics API fails to reform ad-tracking.)

Google's Protected Audience API

While Topics provides businesses with the ability to tap into predefined audiences, Google's Protected Audience API (formerly known as FLEDGE) helps them find and target custom audiences. The Protected Audience API enables on-device auctions by the browser and chooses relevant ads from websites the user has visited. Once a user visits an advertiser's website, the browser receives a request asking it to join an "interest group." An interest group represents a group of people with common interests, corresponding to a remarketing list. When the user visits a site displaying ads, an ad auction runs on the user's device and the ad associated with the winning bid is displayed to the user. This proposal seeks to ensure that information regarding user interests remains on their browser and does not reach advertisers or AdTech platforms. (Chrome Developers Privacy Sandbox: FLEDGE.)

Apple's SKAd Network

As Apple's new ATT Framework reduced advertisers' ability to track its device users at scale, the company introduced the SKAdNetwork, which:

- Attributes impressions and clicks to app installs on iOS apps. The attribution process happens in the App Store before verification on Apple's servers, cleansing data of anything that could identify an individual before sharing it with the ad network or platform.
- Shares conversion data with advertisers without revealing any user-level or device-level data.
- Engages multiple advertisers to simultaneously bid on ad space.
- Requires networks to register with Apple and developers to configure apps to be compatible with these networks.

Apple released version 4.0 of the SKAdNetwork in October 2022, which provides advertisers with improved campaign measurement, engagement and conversion metrics, and access to web-to-app attribution. (Apple App Store: Attributing ads with SKAdNetwork and Private Click Measurement.)

Advertisers using the SKAdNetwork do not need to obtain user consent through the ATT Framework unless they directly engage in tracking through their app (Apple App Store: Attributing ads with SKAdNetwork and Private Click Measurement). Importantly, the ATT Framework broadly defines tracking as the act of linking user or device data collected from one app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising. This includes:

- Sharing device location data or email lists with a data broker.
- Sharing a list of emails, advertising IDs, or other IDs with a third-party advertising network.
- Placing a third-party software development kit in an app that combines user data from the company's app with user data from other developers' apps for targeted advertising.

(Apple: If an app asks to track your activity.)

First-Party Data

Businesses collect first-party data directly from their own consumers' activities and browsing history, such as their intent to purchase, browsing behavior, and transaction history. Many advertisers and website publishers already collect first-party data through their direct relationships with users, with different tools facilitating these relationships based on the technology and value exchange at play. Since first-party data can provide advertisers with unique insight into their target audiences, first-party data tools and solutions are quickly emerging as key alternatives to third-party cookies. Many AdTech companies now provide first-party data tools and services to businesses as privacy-compliant advertising solutions. Businesses developing a first-party data strategy should evaluate different options, as set out below.

Walled Gardens

These ecosystems ensure users do not export personal information while traveling among a family of sites. An operator controls all operations within an ecosystem, such as the Apple App Store or Google Play Store, a social media site like Twitter, or a collaboration platform like Slack. Walled gardens offer a straightforward approach to monetizing data in a privacy-compliant manner since data flows directly from authenticated users. Walled gardens are further supported by data clean rooms (see Data Clean Rooms).

Data Clean Rooms

As first-party data sets emerge as a key alternatives to traditional identifiers like third-party cookies, Data Clean Rooms (DCRs) are quickly gaining traction as a solution enabling collaboration between various stakeholders. DCRs provide a secure environment where advertisers, website publishers, tech platforms, data providers, and AdTech vendors can leverage first party data for audience activation and data enrichment, optimization, and measurement. DCRs accomplish these objectives through a combination of data isolation from DCR participants, privacy enhancing technologies (PETs) such as encryption, privacy controls like data access limitations, and access controls.

Google, Meta, and Amazon initially piloted DCRs, which anonymized personal information to further support each walled garden's ad products. This type of DCR supplements a walled garden to "match" brand targeting with the publisher's consumer data by using ID-based matching to in theory create an anonymous ID. However, different types of DCRs provide different services, which has caused some confusion in the industry. Both Google and Amazon have since launched standalone DCRs accessible by third parties outside of their respective walled gardens and independent from their respective proprietary data. (AdExchanger: Why 2023 Is A Pivotal Year For Indie Data Clean Rooms.)

Importantly, whether an ID is truly anonymous, as opposed to pseudonymous, depends on the details. Most privacy laws only consider data to be anonymous, and no longer constituting personal information, if the specific data subject is not or is no longer identifiable. However, merely processing personal information in a manner that renders it no longer attributable to a specific consumer without the use of additional information, combined with other safeguards, makes the information pseudonymous, which most privacy laws still consider personal information. For example, the CCPA Regulations provide that businesses should treat opt-out preference signals as valid requests to opt-out for that browser or device and any consumer profile associated with it, including pseudonymous profiles (Cal. Civ. Code § 7025(c)(1)-(2)).

With a singular post-cookie solution still out of reach, many independent DCR companies have emerged to provide clean room services without a publisher's treasure trove of first-party data. These independent DCRs can partner directly with ad buyers and sellers to commingle advertiser and publisher data in a privacy-compliant manner, anonymously leveraging third-party data sets to further augment tracking and measurement. Multiple parties can use DCRs simultaneously to store and compare data without sharing personal information through analysis of data set overlaps, a process called model-based matching.

The rise in popularity of DCRs has highlighted the need for industry standards and interoperability between vendors. In February 2023, the IAB Tech Lab released its DCR Guidance and Recommended Practices for public comment (IAB Tech Lab: IAB Tech Lab Launches Data Clean Room Standards Portfolio for Public Comment). The public comment period ended on April 17, 2023.

Personalization

To build user trust, advertisers and website publishers are testing direct consumer communication as a way to achieve privacy compliance and provide a personalized and seamless browsing experience. Consumer surveys, preference centers, and polls can yield first-party data that consumers voluntarily and deliberately share. Google has also created its own website publisher-provided IDs to track authenticated users and their preferences across a single website publisher's offerings.

Consumer Relationships

At the center of all first-party data strategies are transactions in which businesses provide products or services that in turn give them direct access to consumers. Historically cookie-less relationships established by connected TV providers (like Roku and Google Chromecast) and streaming platforms (like Netflix, Hulu, and Spotify) provide a wealth of first-party data that will become even more valuable in the post-cookie ecosystem. Website publishers have also leveraged first-party data through seller-defined audiences, where they can scale anonymized first-party data sets across browser, app, video-delivery, and connected TV environments, rather than relying on external systems that aggregate and normalize audience data points across publisher domains (AdExchanger: Buyers Are Dragging Their Heels On Seller-Defined Audiences Over A Lack Of Transparency). Website publishers should plan to leverage their data across all devices to minimize duplicated reach and provide subscribers with more meaningful ad experiences.

Consent

Advertisers should consider obtaining user consent as part of their future data strategy to account for cross-platform insights. As the AdTech industry embraces targeting through first-party data, companies should be mindful of differing consent requirements when upgrading their user experiences. Obtaining consent from all consumers globally can simplify the process for website publishers, but it may also limit the addressable audience pool. Companies can utilize in-house or third-party CMPs to achieve user experience personalization and remain compliant with global data privacy laws and regulations.

Alternative Identifiers

In addition to leveraging first-party data, advertisers and website publishers have been exploring evolved, third-party alternative identifiers to replicate third-party cookie functionality in a more privacy friendly manner. These identifiers can be categorized as probabilistic and deterministic depending on the data that they use. (The Media Grid: A Guide to Alternative IDs in the Post-Cookie World.)

Businesses should use caution before relying on these identifiers, as their effectiveness can vary based on their implementation, usage policies, and adherence to privacy regulations. For example, businesses subject to the GDPR will still need to provide appropriate notice of and transparency into why they process personal data. This includes having a legal basis for the processing, obtaining consent, and providing consumers with the right to object to the processing and the ability to access, correct, and delete their captured data. Businesses subject to the U.S. state comprehensive privacy laws, like the CCPA, must also have the ability to link these alternative identifiers to consumer profiles to honor opt-out requests. Moreover, as recent FTC guidance and enforcement actions have made clear that hashing, or converting identifiers into a sequence of letters and numbers through cryptography, does not adequately protect consumer privacy if another party can reverse the hashing or otherwise identify the individual user (FTC Business Blog: FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises and Legal Update, FTC Announces Proposed Order Against BetterHelp for Revealing Consumers' Health Data for Targeted Advertising).

Probabilistic Identifiers

Probabilistic identifiers attempt to approximate user identity without relying on any first-party data. Instead, they typically rely on a range of signals collected across multiple channels to best approximate who a user might be. These signals serve as data points and may include, for example, a user's IP address, device type, screen resolution, or operating system. Notably, privacy advocates have raised concerns that certain probabilistic solutions combine device attributes without a user's consent to create a unique identifier. Critics have also pointed out that current laws fail to provide applicable guidance on probabilistic identifiers and how to mitigate the resulting privacy concerns. For example, the CCPA defines probabilistic identifier as the identification of a consumer or their device to a degree of certainty of more probable than not, based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information (Cal. Civ. Code § 1798.140(x)). This implies that identification accuracy of a consumer or their device above 50% probability would be considered probabilistic, and can be made with any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information. This could include first-party data, which makes the CCPA's probabilistic identifiers begin to look more like deterministic identifiers (see Deterministic Identifiers).

Despite these concerns, ID5 has emerged as a leading probabilistic solution, that among other things, provides website publishers with the ability to outsource their cookie-syncing process through a universal identifier. ID5 stores its encrypted IDs on website publishers' first-party cookies. These IDs are then shared by the media owner with their AdTech partners and used by advertisers for targeting and measurement through ID5s's Identity Cloud platform. (ID5: ID5 IdentityCloud.)

Lotame's Panorama ID is another emerging probabilistic solution that merges device identifiers, individual behaviors, and privacy choices to build identifiers using inputs from web, mobile, connected TV, and user-level IDs (Lotame: Panorama ID).

Deterministic Identifiers

Deterministic identifiers rely on user personal information, like an email address, that is then hashed or anonymized for the matching and bidding processes. For example, leading supply-side platform the Trade Desk developed the Unified 2.0 ID (UID 2.0), which collects authenticated user personal information and consent preferences. The UID 2.0 then creates an encrypted form of this data known as a UID 2.0 Token and passes it along on the supply-side platform. The demand-side platforms decrypt these UID 2.0 Tokens and bid accordingly, or block use of the UID 2.0 Token if a user has opted out. While The Trade Desk is building support for its identity solution from Omnicom Media Group and Connected TV (CTV) publishers such as AMC, Fubo, and Tube, the company is simultaneously searching for an independent administrator to take on the technology's stewardship. (theTradeDesk: Unified ID 2.0.)

RampID (formerly known as IdentityLink) is another solution in which a publisher assigns an identifier upon user e-mail authentication after encrypting and hashing this information. RampID connects this inventory to first-, second-, and third-party data for activation, but individuals are only addressable by RampID on authenticated domains. (LiveRamp: RampID Methodology.)

Contextual Advertising

Contextual advertising places advertisements based on a website's content, a user's current location, or other characteristics to deliver relevant ads without relying on a user's past behavior. Contextual advertisements are generally targeted to sites using a pre-determined category, such as a keyword or a website topic, that a crawler that scans and classifies web pages collects. When a user visits a site, it communicates its content category to the ad server, which matches it to an ad corresponding to the keyword or topic. Because contextual advertising does not typically leverage user personal information to deliver an ad, it is not generally subject to data protection laws and regulations.

However, contextual advertising is not a panacea, as the EU ePrivacy Directive's cookie requirements would still apply. While contextual ads are generally an easier and more affordable alternative than behavioral ad placements, solely contextual campaigns may not achieve the size and reach of behavioral advertising. For that reason, many advertisers are already incorporating personal information into the delivery or targeting of their contextual ad campaigns. This practice inevitably triggers the data protection laws that contextual advertising was originally intended to avoid.

Best Practices to Prepare for the Post-Third-Party Cookie World

Advertisers and website publishers should consider a multi-pronged approach when developing their post-cookie strategy, as it is unlikely that a one-size-fits-all solution will exist. These businesses should evaluate a combination of tools that best match their current data sets and prospective marketing plans while considering the evolving privacy-conscious regulatory and technological frameworks.

To that end, businesses should take steps now to best position themselves for a post-cookie world, including to:

- Understand their current reliance on third-party cookies, specifically:
  - what role these cookies play in their current advertising strategy; and
  - to what extent their marketing dollars and impressions are tied to behavioral targeting.
- Conduct an audit to assess the scope and quality of the first-party data they hold, as many advertisers and website publishers may not know the extent of their first party data collection.
- Invest in data management platforms and technologies to organize their first-party data assets and obtain valid consent from current users to collect and use their personal information.
- Use existing and upcoming campaigns to grow their first-party audience and first-party data through email, newsletters, surveys, promotions, digital events, loyalty and rewards programs, or sign-up campaigns to increase their first-party data pool and capture audience interest and demographic data.
- Before onboarding first-party data into a DCR to connect anonymized data from multiple parties, ensure that their DCR strategy and implementation incorporates privacy-enhancing technologies and privacy control mechanisms to meet legal and regulatory requirements.
- Weave contextual advertising into their current and post-cookie marketing strategies to complement their first-party, DCR, and alternative ID strategies. Businesses should identify key topical categories for specific audience segments and combine them with brand safety and suitability tools, inclusion and exclusions lists and keywords, while leveraging sentient and contextual AI. However, businesses should work with privacy counsel to ensure they do not trigger potential regulatory obligations. For example, if a contextual advertising strategy incorporates personal information, it may fall under the CCPA's definition of sale or sharing.
- Continuously monitor the development of third-party cookie alternatives such as Google's Topics and Protected Audience APIs and Apple's SKAdNetwork.
- Adopt a privacy by design mindset and approach throughout their business with an emphasis on consumer privacy. This is particularly important in the product and service development area of the business.
- Consider adopting consent-based approaches when developing a post-third-party cookie strategy to help ensure compliance with global and US state privacy laws and consistency with the most relevant emerging cookie-alternative strategies and tools.

About Practical Law
Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.