AdRoll

Zero- and First-Party Data Strategies

for Retargeting With Fewer Third-Party Cookies
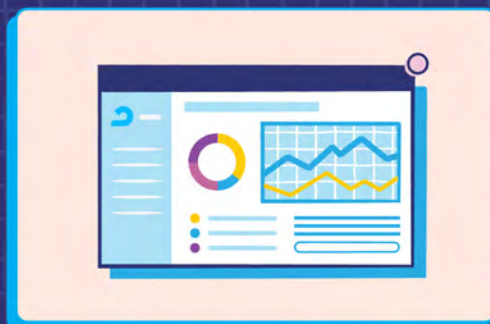
AdRoll

Table of Contents

Foreword

The planned shift away from third party cookies on Chrome has been looming over digital advertising for years. As we approach the eventual lessening of cookies, the prospect can be a bit unnerving. What does this mean for my business? Will my campaigns continue to run? What can I do to prepare to ensure the best outcome for my business?

While one technical aspect of digital advertising is being changed, the core requirement of showing the right ad, to the right audience, at the right time still remains unchanged. This advanced guide is meant to help calm concerns and give the savvy marketer key information and concrete steps to take to help ensure a successful and smooth transition.

Rob Myers
Sr. Product Manager, Advertising
AdRoll

Defining the Differences Between Zero- and First-Party Data

As the industry moves away from third-party cookies (3PCs), zero-party and first-party data play an increasingly important role in campaign targeting, retargeting, and personalization. As a result, it's important to understand the difference between the two.

First-party data is information collected passively from customers and their interactions with your business. It is often collected using first-party cookies (1PCs) and tracks user activity or behaviors on your website or your mobile app, including page views, video completion rates, product purchases, and other on-site actions.

Zero-party data, however, is a relatively new subcategory of first-party data that was made popular by Forrester.

Businesses collect zero-party data by asking customers to provide their information through forms, account creation, newsletter subscription opt-ins, and loyalty program enrollment.

These activities may ask for demographic or firmographic data, along with qualitative data like why they chose to purchase or how they plan to use your product. Zero-party data may include:

- **Personally identifiable information (PII)** like name, email, address, phone number
- **Demographic data**
- **Preferences**

First-party data is collected passively by observing customers and typically focuses heavily on website activity. Zero-party data is solicited by the brand and provided directly by the customer.

Since customers directly provide zero-party data, it may offer a higher degree of accuracy than first-party data. First-party data only captures what a brand can observe through customer activity, which can be susceptible to inaccuracies.

	Zero-Party Data	**First-Party Data**
Collection Method	• Receive data directly from users • Opt-in and lead-generation forms	• Observed from user interactions and online behaviors • Passive
Types of Data Collected	• Brand-relevant data, including qualifying information • Name • Email address • Phone number	• User behavior and observed preference • Pages viewed • Products viewed • Items added to cart
Stage of Customer Journey Collection Happens	• Often occurs once some trust is built and value is "worth" exchanging by the customer • Can happen during early stages of the funnel with right incentives	• Collected throughout the customer journey once consent is granted, if required by local privacy regulations • Can happen during initial site visit
Pros	• Can include qualifying data that may be hard to gather otherwise • Can provide highly accurate, self-reported data from users • Invaluable for retargeting and personalization	• Can collect observational data users may not share on a lead form • User activity and preferences can be used to create relevant and timely retargeting campaigns
Cons	• Customers must build trust first, takes longer to acquire • User consent can be revoked	• Is at risk for occasional inaccuracies, such as multiple users on a single device • Users can opt out or clear their cookies at any time

Gathering Zero- and First-Party Data Effectively

Because many individuals will likely opt out of 3PCs when given the choice, gathering zero and first-party data is key. When gathering zero- and first-party data, it's important to know what information to collect and how to do so. Let's discuss the strategies, considerations, and best practices for collecting zero- and first-party data effectively.

What Kinds of Data Should I Collect?

The most valuable data points for marketers include:

- **Username**
- **Email addresses**
- **User preferences**
- **Previous actions, including site activity**
- **Customer information that's relevant to your brand**

Let's talk about that last bullet point. Capturing contact information like email addresses and users' names is table stakes, so go a step further and consider what information is most impactful for your marketing and sales departments. This data can help you learn about your target audience, qualify leads, and create targeted advertising campaigns.

A financial services company, for example, collects data specifically relevant to their services. If you're shopping for a mortgage, the initial interest form requests your name and email address, but will likely also include information fields requesting the following:

- Type of mortgage you're interested in
- Down payment amount
- Estimated cost of the house you want to purchase
- Current credit score
- Current income
- Purchase time frame
- Home location

This information helps the mortgage company best serve customers. Knowing the customer's location, for example, can help pair the customer with a local branch, and certain loan officers may handle different types of mortgages.

Remember, once you have this kind of data, an advertising technology partner like AdRoll can help you activate it across the right marketing channels. We'll talk more about this later on.

How Do I Collect It?

Knowing how to collect zero- and first-party data is just as important as knowing what to collect. Here's what the process looks like.

Ask Directly with On-Site Strategies

The best way to gather zero- and first-party data is to ask for it.

Many regions require user consent for first-party data collection using 1PCs under certain privacy regulations (which we'll discuss in the next section). Because of this, you may be required to ask for permission before automatically tracking user data.

Zero-party data can only be collected when users share it.

Marketers can use on-site pop-ups, widgets, and lead forms to gather zero-party data like users' names, email addresses, and other qualifying information.

Consider Privacy & Consent

Zero-party data can only be obtained when a customer shares it, and some first-party data requires cookie consent.

According to the GDPR, website owners do not need to acquire consent for "strictly necessary cookies," which are necessary for website function. These cookies, for example, may allow you to access secure sections of a website or retain items in your cart as you browse.

The GDPR does require, however, that websites obtain consent from users for all other first-party cookies, including those that store a customer's product or language preferences.

The good news is that unless consent is revoked, advertisers will be able to continue using this data to deliver ads to high-value customers once consent is granted.

A strong cookie consent banner may help you increase the number of users who opt in to first-party tracking by increasing transparency about what data you're collecting.

Build Trust

Trust is perhaps the most crucial factor when capturing first- and zero-party data. You need consent to capture the data, which can then be revoked at any time — users can opt out of your email list and revoke cookie access, for example.

As a result, it's important to abide by your published terms of service and privacy policies. Continue to foster customer relationships by not abusing the information they've shared with you. Instead, use it to deliver more personalized and relevant customer experiences.

You also don't want to misuse data by spamming users. This could include sending unsolicited business communications (including email, phone calls, and SMS messages) that users did not consent to.

Build a Value Exchange

According to one of our experts, Rob Myers, Senior Product Manager of Advertising, one of the biggest challenges regarding zero-party data is that brands are only able to capture it from around 5% of site visitors. This leaves an enormous opportunity to capture data from the remaining 95% of site visitors.

Creating an exchange of value can help incentivize users to participate. Examples of utilizing incentives include:

- Offering free content like eBooks, webinars, or whitepapers if users complete a lead form
- Promoting discounts in exchange for a user's email address or phone number
- Providing access to freemium, standalone tools that support a larger SaaS product
- Highlighting your email newsletter, which could contain valuable product updates or relevant content

The most commonly used strategy for capturing zero-party data is to offer either a first-purchase discount or access to a loyalty program. But remember, you'll get the most lifetime value by considering the entire buyer's journey.

Discounts are relatively low-effort and may only capture users who already have high buyer intent. An ongoing value exchange through content can attract more users at different stages of the buyer's journey.

How to Use Zero- and First-Party Data for Personalization & Targeting

Because of the shift away from third-party cookies (3PCs), zero-party and first-party data is even more critical now than it was in the past.

The good news is that many brands are likely already using both zero- and first-party data in some capacity for personalization and targeting. This chapter will dive deeper into how to leverage this data effectively as businesses look for future-proof tactics that will preserve and enhance retargeting within a privacy-forward advertising ecosystem.

Google Privacy Sandbox

Google's Privacy Sandbox seeks to create a "more private internet." It's an initiative by Google that is creating technology that both protects user

privacy while still giving advertisers the tools needed to create strong, well-targeted campaigns.

A core focus of Privacy Sandbox is reducing cross-app and cross-site tracking, including blocking covert tracking, while still keeping online content free. This includes Google phasing out 3PCs and creating [new web standards](#).

Protected Audiences API

[Protected Audiences API](#) (PAAPI) is a technology stemming from the Privacy Sandbox project. It will serve remarketing and custom audience use cases while ensuring third parties can't track user browsing behavior across different sites.

PAAPI works by allowing advertisers to create "interest groups." When users browse the advertiser's website, they may be added as interest group members. For example, if users are looking at houseplants online, they might be added to a "houseplant interest group." That membership is stored on the user's own device.

Interest groups owners are often demand-side platforms (DSPs)

When that same user visits a publisher site that sells ad space, the publisher's site may trigger an auction, asking for bids from the DSP interest group owners. Advertisers submit bids, and the winning ad then appears on the site, where the user sees it.

The above example is a good simplification of PAAPI segmentation and targeting. In reality, PAAPI is much more complex and will support the same segmentation used today in AdRoll that leverages advertisers' first-party data.

How zero- and first-party data can be used

First-party data can be used to create interest groups within PAAPI.

As an example: If a user visits a page for petite women's jeans, they may be added to a "petite clothing" interest group.

This categorization allows brands and DSPs to identify these user segments in subsequent auctions. Current segmentation will be the same for the API, as no changes are expected to be made that will impact the user experience.

Zero-party data in the form of PII (email, address, phone, etc.) is not currently able to be onboarded to PAAPI or other privacy sandbox solutions. It is important to keep in mind that there is no 1:1 targeting available through PAAPI. As a result, it can be a useful part of an ID-based targeting strategy, but advertisers will need additional retargeting and personalization strategies.

AdRoll's approach

NextRoll has been working with Google and the World Wide Web Consortium (W3C) since 2020 — since Google first announced its plans to phase out third-party cookies in Chrome.

We're actively testing Privacy Sandbox APIs. This testing is currently limited to 1% of Chrome users, and the goal of testing is primarily to verify functionality of the specs in question. We've been using this advanced access to develop solutions around first-party data to help our clients reach their target audiences.

Alternative Identifier: Deterministic IDs

Deterministic IDs rely on a user's PII and are created via authenticated registration events like a user log in. This is most often an email address that's encrypted to keep the actual user anonymous, protecting their digital privacy.

How zero- and first-party data can be used

Email addresses are the primary piece of PII that create most deterministic IDs, so active efforts to collect zero-party data, including email addresses, are essential here.

Once you have an email address and create a deterministic ID for the user, you can track first-party behavioral and interest data attributes to the user's specific deterministic ID. If user A adds products to their cart but doesn't purchase, for example, their online activity will be synced with your CRM. You can then send an abandoned cart email automatically or retarget the user with relevant ads across web or app environments using a DSP that supports the deterministic ID provider technology.

Because deterministic IDs are reliant on PII, they're expected to be limited in terms of scale availability. Users have to want to share their information with you, which is where incentives can come into play. Users also have to share their email information with publishers who sell advertising space on their website(s) or app(s).

That said, deterministic IDs are often highly accurate because the information is coming directly from users themselves.

The primary programmatic advertising activation path for zero-party data is through the use of deterministic IDs, which can then be used to link first-party data observed from the advertiser's website.

AdRoll's Approach

NextRoll has built support for LiveRamp's RampID, which can help reconcile data from multiple sources and sync first-party and zero-party data effectively.

We're currently monitoring the prevalence and adoption of other deterministic IDs across our supply partners, and we plan to support additional IDs as we begin to see critical mass across the ecosystem. Our ultimate goal is being interoperable with all industry-leading IDs.

Alternative Identifier: Probabilistic IDs

Probabilistic IDs rely on multiple cross-channel signals to approximate user identity without the collection of PII from zero-party data.

Probabilistic IDs may rely on the following data points:

- **IP address**
- **Screen resolution**
- **Device type**
- **Operating system**

How zero- and first-party data can be used

Probabilistic ID providers rely on collecting a range of signals to create their specific identifier, most of which come directly from first-party data, including all the data points listed above.

Zero-party data is not typically used to create probabilistic IDs, which do not rely on PII.

Because probabilistic IDs are not reliant on personally identifiable information, the data involved is much easier to collect and more widely available.

That said, probabilistic IDs are also often less accurate compared to deterministic IDs. They also have a lower persistence over time due to browser-readable signals.

There are currently 40+ IDs on the market today, each with varying degrees of prevalence in adoption.

AdRoll's approach

NextRoll has built support for 33Across's probabilistic ID called Lexicon ID.

We're also monitoring the adoption of other probabilistic IDs across our supply partners, with the plan to support additional probabilistic IDs as adoption becomes more prevalent.

Our goal is to build a flexible platform that can easily adopt new IDs as adoption and use merits.

Email Retargeting

Email retargeting is a common tactic that involves sending users emails with relevant content (including discount offers) based on user data, including preferences and actions. If a customer adds an item to their cart but doesn't purchase, for example, you can send that user an email with a coupon code and remind them their cart is waiting.

How zero- and first-party data can be used

Email retargeting campaigns often combine deterministic IDs from zero-party data and first-party behavioral and session data to create highly personalized experiences for each user. The zero-party data is critical to connect with users through email, and the first-party session data will determine what content users see in a retargeting email.

Users will receive campaigns based on recent and historical preferences and activity, and the use of email autoresponders can ensure the campaigns are timely and relevant.

AdRoll's Approach

AdRoll's email retargeting solution helps advertisers build strong, personalized email campaigns, including autoresponder campaigns.

Advertisers can also set up cross-channel campaigns that include email retargeting — all from a single, easy-to-use platform.

Leveraging Tactics Together to Maximize the Value of Retargeting

We've discussed different future-proof tactics that will preserve and enhance retargeting the shift away from 3PCs, and how zero-party and/or first-party data apply to each tactic.

While the future state of retargeting with fewer 3PCs is still evolving, it is more than likely that no single tactic alone will emerge as a silver bullet solve-all. Rather advertisers will need to leverage each of these tactics in concert with one another to maximize the value of their retargeting efforts.

Now let's take a look at how zero- and first-party data collection strategies, plus leveraging multiple retargeting tactics, might look relative to a full-funnel marketing effort.

They use the following strategies to reach cold audiences:

- Google Ads targeting placements for keywords like "buy first house," "how to get a mortgage," and "private mortgage company"
- Facebook Ads to generate interest using location targeting
- CTV ad campaigns to generate brand awareness using interest targeting
- Paid promotions with relevant social media influencers and bloggers, including real estate companies or financial advisors

Once users land on their website, they use these tactics to collect zero- and first-party data:

- Referral programs with local real estate agents
- Provide a value exchange for zero-party data like a user's email. Examples could include a discount code, free estimate, potential qualification, or current interest rates using a simple lead form
    - Offer access to high-value content like eBooks or courses like "first-time home buyer discounts," "seller checklists," and mortgage calculators
- Get permission to track user activity with first-party cookies
- Track observable on-site activity like products viewed, pages viewed, et cetera
- Follow up with personalized email campaigns based on user activity and data

They then use retargeting and personalization strategies like the following:

- Create retargeting campaigns to offer free consultation calls with a loan officer using the following tactics across desktop and mobile web environments:
    - Google's Protected Audience API (PAAPI) campaign
    - Deterministic ID campaign
    - Probabilistic ID campaign
- Personalize the customer's website experience to show them relevant offers or to continue the application process

AdRoll's Approach to Future-Proof Retargeting

As we consider the level of effort required to set up and manage multiple campaigns using each of the future-proof tactics mentioned above, we know a fair amount of coordination between ad operations and third-party ID vendors will be required. This includes:

- Configuring interest groups and bid logic for creatives in PAAPI
- Testing each deterministic and/or probabilistic ID to determine which has sufficient scale and performs best for you (not to mention finalize commercials if needed)
- Setting up and managing multiple campaigns for each ID provider
- Allocating and reallocating budgets across campaigns to optimize for reach and performance

Instead, advertisers can partner with AdRoll and we'll do all the heavy lifting. As early leaders helping to develop the Privacy Sandbox APIs, we'll manage creation of interest groups and bid logic plus optimization of creatives in PAAPI without adding additional day-to-day work for the marketer.

We'll eliminate the guesswork of deciding which IDs to select for your campaign by supporting the leading IDs and using them to best meet your campaign's goals. We'll also determine how much budget to allocate to any given tactic using our AI bidding algorithm, BidIQ. We'll help you leverage your zero-party and first-party data to more effectively reach your target audience throughout the entire sales funnel.
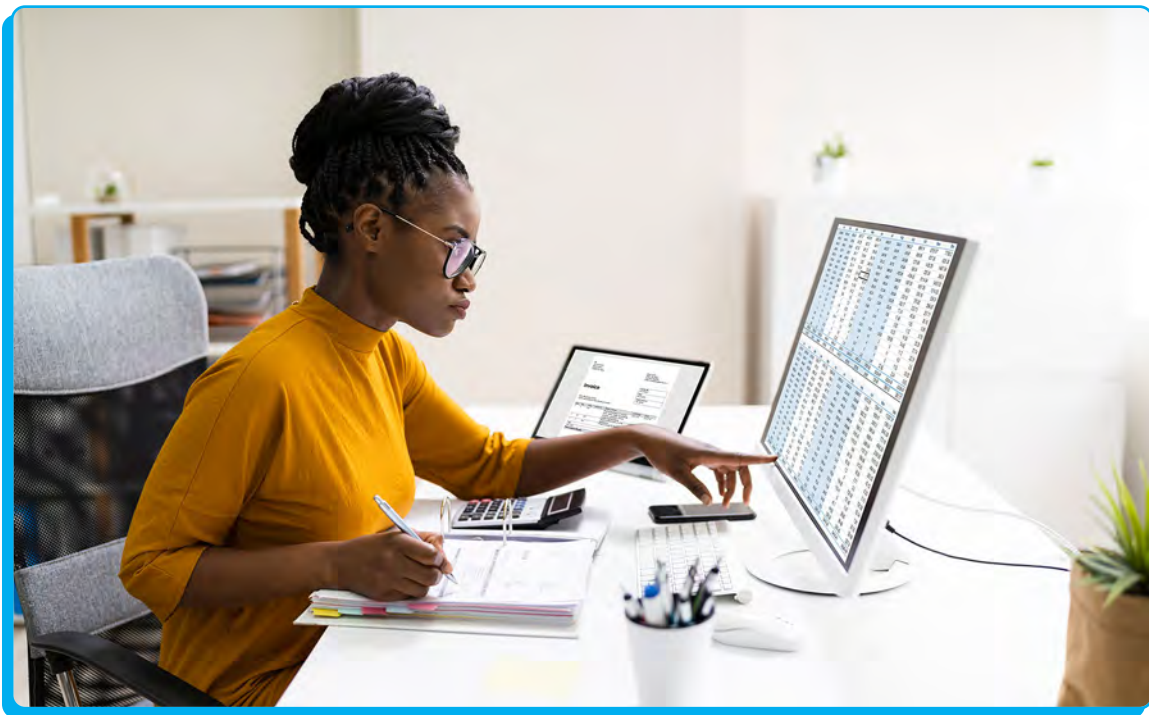
Preparing for a World With Fewer 3PCs With Your Ad Provider

The shift away from 3PCs is a massive change from the advertising landscape of the past, and it's important that ad providers are prepared. 3PCs are, by nature, pervasive and sticky, but the increasing cost of privacy is that some currently reachable audience members will be lost.

This leaves most brands wondering the same thing: "What can I do today to ensure I'm prepared for a world with fewer third-party cookies?"

For starters, brands should start or continue collecting more zero-party data and storing it in CRMs or CDPs.

Additionally, brands should consider testing emerging future-proof tactics

to determine the impact each will have on performance. It's important, however, to also consider factors like market adoption and technical readiness of each tactic to determine whether "impactful testing" can be done at this time.

The Privacy Sandbox APIs are still in the early phase of industry testing, with only 1% of Chrome browsers moved off of third party cookies, and furthermore has had limited publisher participation. While testing has indeed been ongoing since 2020, much of this has been centered around functional aspects of the API (e.g., end-to-end systems testing), and feedback has been used to evolve the technical specifications. Without representative supply adoption and knowledge of what the end specs will support, any tests run will be limited in their ability to measure future impact of a world with fewer 3PCs.

Deterministic and probabilistic IDs face a somewhat similar predicament with respect to market adoption. While there are less technical aspects to consider compared to Privacy Sandbox API, there are 40+ alternative identifiers on the market and varying degrees of adoption by publishers.

The availability of 3PCs further limits the ability to measure the future impact of shifting away from them by creating signal noise (i.e., when two or more IDs are present). This can create a false perception of scale, as 3PCs are often used to persist deterministic and probabilistic IDs cross site. For these reasons, individual advertiser testing of alternative IDs also has a limited ability to measure future performance of these solutions.

While "impactful testing" of Privacy Sandbox APIs and alternative identifiers is limited by the current lack of market adoption, and in some cases technical readiness, there are ways to gauge whether your current ad provider is prepared to help you navigate these tactics in a privacy-forward advertising ecosystem.

To ensure your ad provider is ready to help you in a world with fewer 3PCs, you can ask these questions:

- Have you been involved in the W3C and the development of the Privacy Sandbox API specs?
- What level of testing have you done to date on the Privacy Sandbox APIs?

- Which APIs have been tested?
- How will your attribution reporting be impacted by by fewer 3PCs?
- Which deterministic IDs and/or probabilistic IDs do you support today and why?
    - Which do you plan to support in the future?
- Which systems and functionalities are 3PC dependent?
    - How are you future-proofing these systems?
    - What systems will be drastically impacted or not future-proofable?
- What approach(es) will you take to future-proof your technology?

As you're assessing your ad provider, watch for these potential red flags:

- They're unfamiliar with the extent of 3PC changes, or brush off concerns about the potential severity of impact.
- They don't already have a plan in place to account for the loss of reachable audiences from from 3PC changes.
- Collecting and maintaining user privacy and consent aren't core considerations in their strategies.
- They don't have methods in place to leverage first- and zero-party data for retargeting, interest-based targeting, or full-funnel campaigns.
- They aren't able to provide specifics about campaign attribution, performance tracking, and optimization.
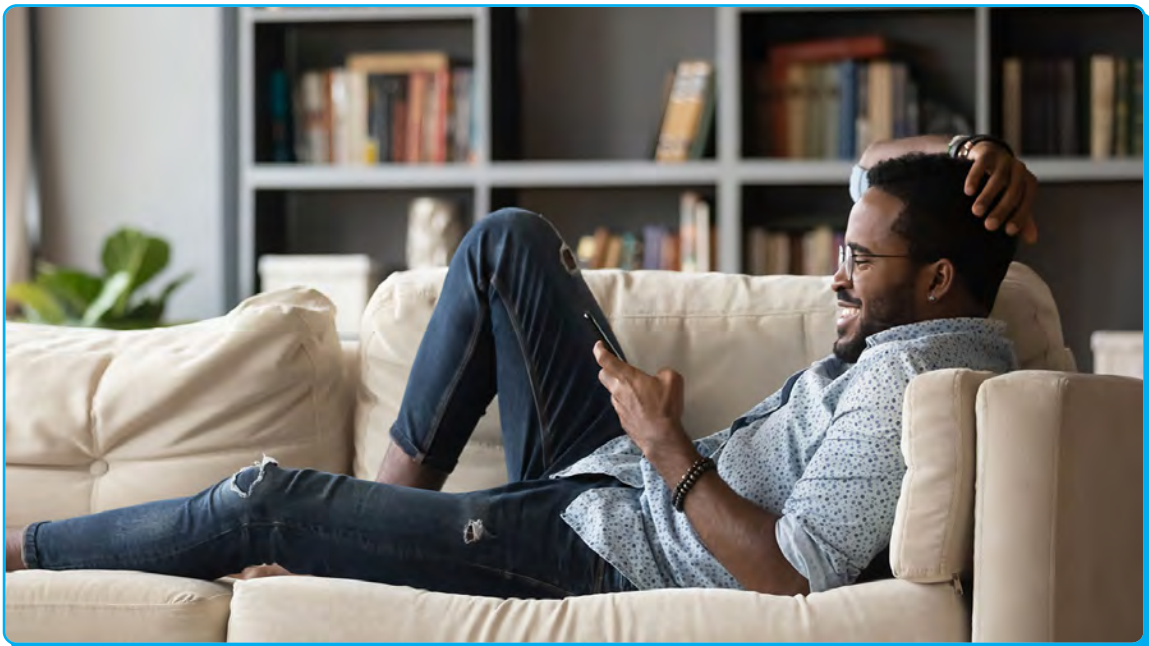
How AdRoll is Paving the Way to a Future of Intentional Advertising

AdRoll helps D2C businesses run, measure, and optimize full-funnel, multi-channel campaigns — and we're fully prepared for a privacy-forward advertising ecosystem.

We're dedicated to playing an active role in developing new advertising solutions and increasing support for them, all so you can continue reaching your target audience and hitting your ROAS goals.

Along with preserving the current retargeting functionality as listed above, AdRoll will continue to provide non-person based targeting through:

- Continued support for prospecting campaigns
- Continued support for contextual campaigns
- Testing of the Privacy Sandbox Topics API
- Continued support for CRM targeting via IDs
- Continued support for attribute targeting
- And more…We are always looking for more compelling ways to put the right ad in the right place at the right time

Learn more about how AdRoll can help you adapt to a world with fewer 3PCs and more zero- and first-party data solutions. Get in touch with our sales team here.

AdRoll

Follow us for more!

AdRoll is a marketing and advertising platform that helps B2C businesses run, measure, and optimize multi-channel, full funnel campaigns. Powered by industry-leading AI and automation, the AdRoll platform's machine learning analyzes both real-time and historical data to drive traffic and sales. AdRoll helps customers generate more than $246 billion in sales annually and has been used by over 120,000 brands since 2006. AdRoll is a division of NextRoll, Inc. Get started today at www.adroll.com.