



Digital Advertising in the COOKIELESS WORLD

Lorem ipsum dolor sit amet



Introduction

For several years, browsers and government regulators have been ringing the death knell for third-party cookies (small pieces of code installed on a user's browser, by a domain they've never visited, to track behavior across websites).

Third-party cookies and data sharing have long been the backbone of digital advertising. We've all seen them in action: we search for a pair of sneakers, and suddenly sneaker ads are following us from site to site.

This type of retargeting has been increasingly off-putting to users; dredging up questions of who, exactly, has access to this personal data and how is it being used? It's a dynamic that has cast third-party cookies in a less than flattering light: seen, at best, as a murky approach to data collection, and at worst, an invasion of privacy.

In 2023, Apple announced new **privacy measures** for its iOS 17 update. In addition to users having to explicitly grant app developers permission to share their phone's unique identifier (IDFA) for tracking and advertising purposes (beginning with iOS 14), iOS 17 includes mail privacy protection, safety check, location services, and updated passkeys – the phishing-resistant password replacement that allows users to log in without worrying that their passwords might get stolen.

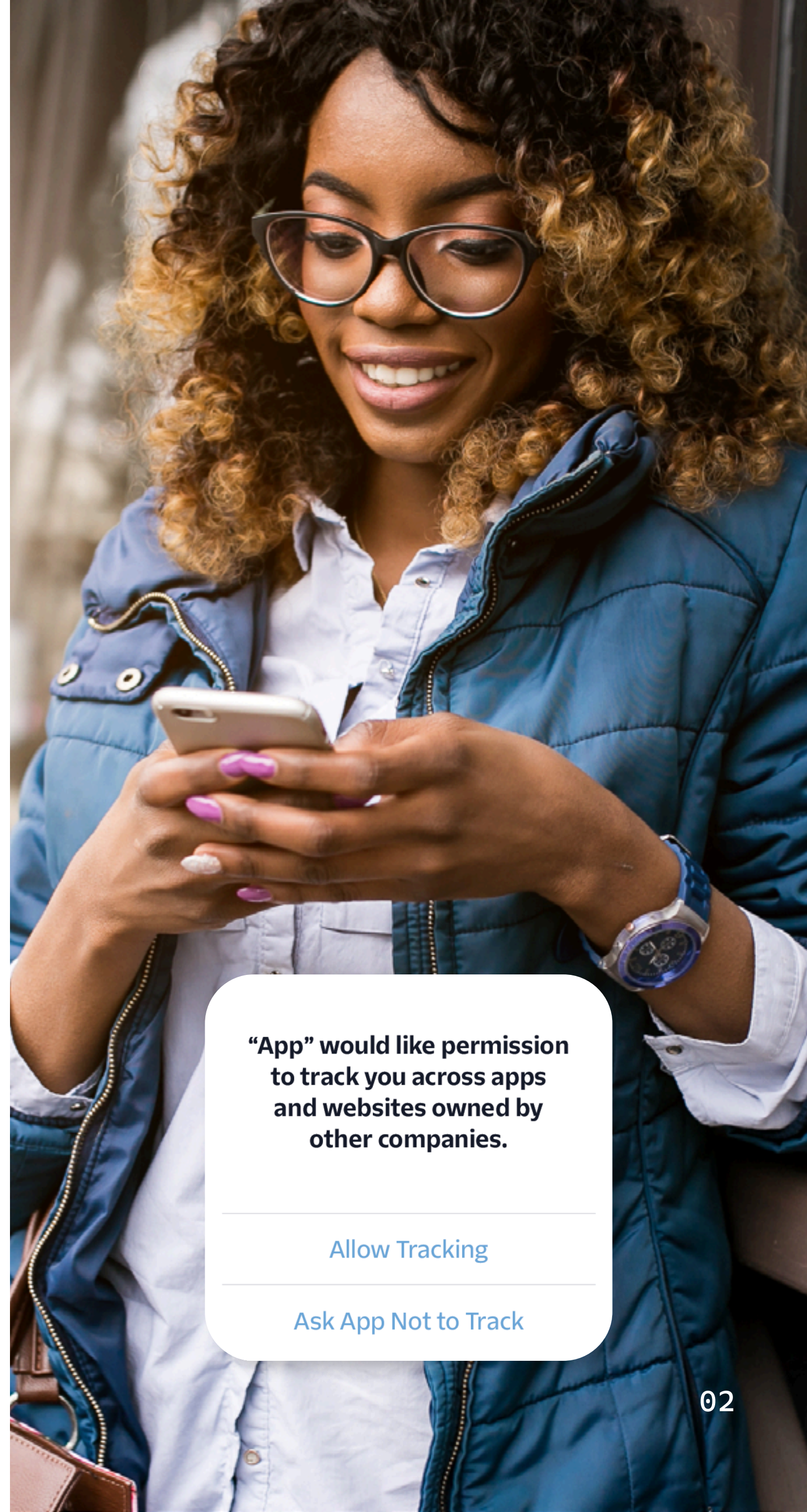
While Google initially planned to deprecate third-party cookies in Chrome, it has since backpedaled. Users can continue to manage third-party cookie settings through Chrome's existing Privacy and Security controls.

The reversal came in response to ongoing regulatory scrutiny—particularly from the UK's Competition and Markets Authority—as well as critical feedback from advertisers and other industry stakeholders.

Despite stepping back from its original approach, Google is still exploring alternative privacy-focused technologies, such as IP Protection for Chrome's Incognito mode, to enhance user control over personal data.

The uncertainty of third-party cookies doesn't automatically mean disaster for digital advertisers. In fact, there's a better, more ethical way forward with first-party data.

In this guide, we cover how a Customer Data Platform (CDP) will be pivotal in this switch to a privacy-first digital advertising landscape.



“App” would like permission to track you across apps and websites owned by other companies.

[Allow Tracking](#)

[Ask App Not to Track](#)

TABLE OF CONTENTS

How browsers are handling user privacy	2
Who’s impacted by the end of third-party cookies?	5
The different types of data	9
First, second, third, and zero-party data	11
CDPs vs. DMPs	16
The benefits of first-party data for advertisers	17
Why CDPs are pivotal in a privacy-first world	17
About Twilio Segment	17
Recommended Reading	17

HOW BROWSERS ARE HANDLING USER PRIVACY

01



Apple

- It began in 2020 when Apple announced that its iOS 14 update will require app developers to explicitly get permission from users to track their IDFA (their phone's unique identifier) with App Tracking Transparency. (Before users had to opt out of IDFA tracking, now they have to opt in.)
- In 2023, Apple announced its iOS 17 update that also includes mail privacy protection, safety check, location services, and updated passkeys.

Google

- **March 2020:** Google announced plans to phase out third-party cookies in Chrome by 2022 as part of the Privacy Sandbox initiative.
- **June 2021:** The deprecation timeline was delayed to 2023 (then, later, to 2024).
- **April 2024:** Google postponed the deprecation again, aiming to begin in early 2025, contingent on regulatory approval from the UK's Competition and Markets Authority (CMA) and Information Commissioner's Office (ICO).
- **July 2024:** Google announced it would not proceed with deprecating third-party cookies. Instead, users would manage cookie settings through existing Chrome privacy controls.

Mozilla

- In 2020, Mozilla announced Total Cookie Protection, which places website cookies in their own, distinct cookie jar to prevent cross-site tracking.
- In 2024, Mozilla introduced a paid subscription privacy monitoring service called **Mozilla Monitor Plus** that will automatically keep a lookout for your information at over 190 sites where brokers sell information they've gathered from online sources like social media sites, apps, and browser trackers; when your info is found, the service will automatically try to get it removed.



WHO'S IMPACTED BY THE END OF THIRD-PARTY COOKIES?

02



The end of third-party cookies represents a fundamental shift in digital advertising. Let's break down the key players involved, and how they're impacted.

Publishers

In digital advertising, there are two types of publishers to consider:

- Media companies (like The New York Times, CNN, Vice)
- Tech giants (like Google, Amazon, Meta)

Put simply, publishers display ads on their digital space: whether it's natively in content, sponsored in social media feeds, a paid search result, and so on. This is how most media publishers have monetized their content – relying on ad revenue to stay alive.

That's why there's been a push among media publishers (like The New York Times, The Washington Post, etc.) to strengthen other revenue streams outside of digital advertising. Usually, by instituting paywalls to grow subscription rates.

But to future-proof their business, media publishers need to take control of their own data.

This is why more forward-thinking media companies plan on (or have already started) bolstering their first-party data collection to power their own revenue stream.

Looking ahead, **78% of publishers believe removing third-party cookies will make their audience data “more valuable.”** According to Digiday, the removal of third-party cookies will allow publishers to gain additional technical protections against data leakage while finding new paths to audience revenue with first-party data.



78% of publishers believe removing third-party cookies will make their audience data “more valuable.”

Tech giants

Google and Facebook have long been powerhouses in **digital advertising** (representing 39% and 18% of ad revenues in the US, in 2023), with Amazon carving out a space in this top tier with 7% and TikTok gaining market share with 2.3%.

They've structured themselves as "walled gardens" or closed ecosystems – collecting a wealth of first-party data from their massive user bases, which stays within the confines of their organization.

For quick context: Facebook has roughly **3 billion** daily active users, while Google has over **1.8 billion Gmail** users worldwide (and more than **2.7 billion** logged-in YouTube users a month). Whenever those users are logged in to these platforms, they're generating first-party data (e.g., social media posts they engage with, search history, etc.).

Then there's Amazon, which currently represents nearly **50% of the e-commerce market** share in the US. Consumers on Amazon have incredibly high intent, providing the company with a not-so-secret ace in the hole of purchase data (which feeds the company's rapid experimentation and spot-on product recommendations).

So while these tech companies may feel an initial tremor following the depreciation of third-party cookies and IDFA, they already have a solid infrastructure for success with their troves of first-party data.

Publishers and advertisers need to think about the post-cookie world. How do we get people to choose to participate? We are seeing more publishers move to subscription models. This isn't just about money, but it's about having higher quality data that better understands the customer, the content they consume, and the things that may interest them. This is only one of the pivots, but any business in any industry needs to think about why someone would want to expose their data – what real value is being created?

Daniel Newman,
Principal Analyst at Futurum

Advertisers

For digital advertisers, the status quo has been to track site and app users by allowing ad networks and Ad Tech companies to place third-party cookies on their properties; essentially giving up control over their data.

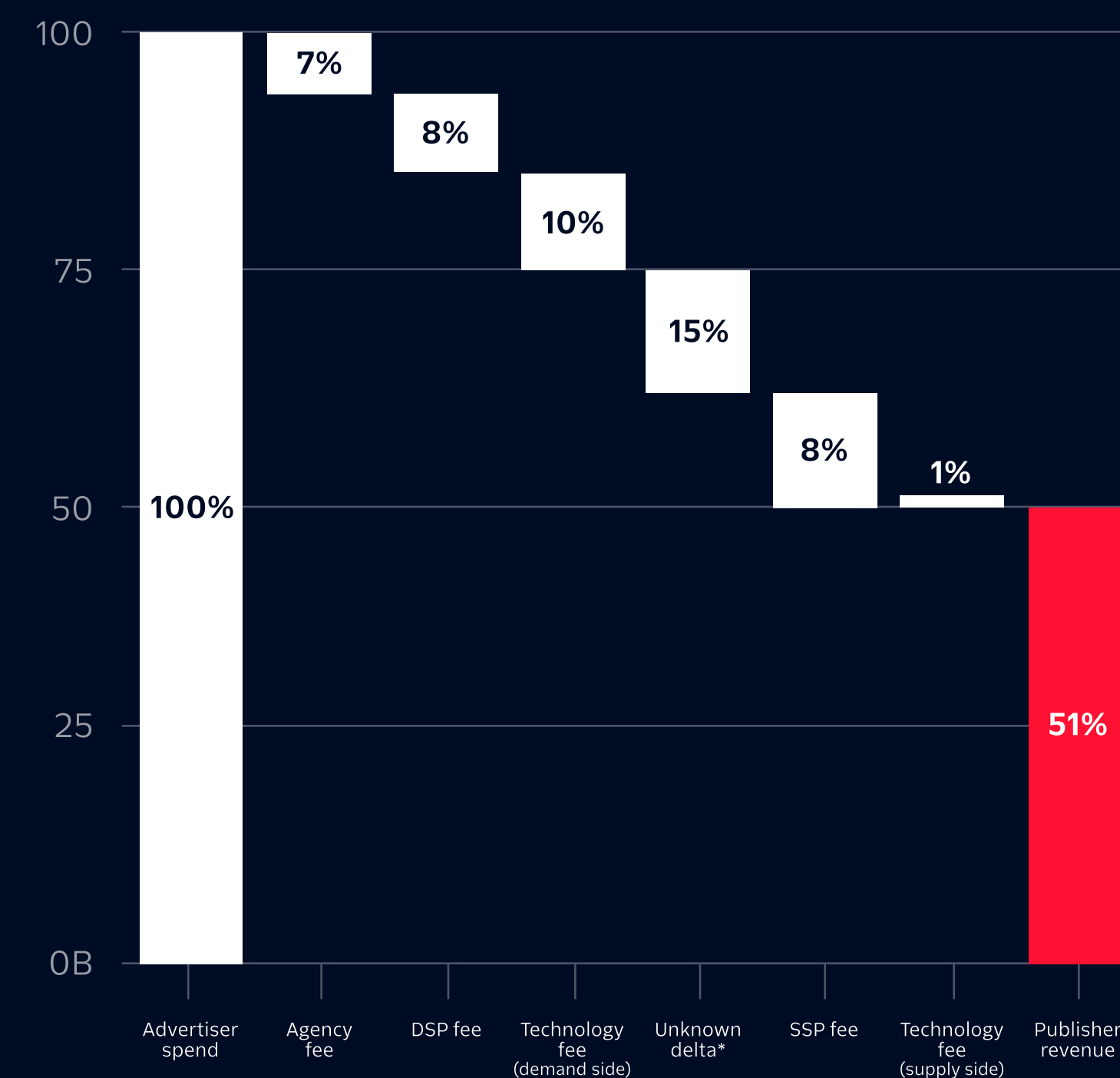
The ban on third-party cookies means that most advertisers will have to rework entire strategies. But maybe it's about time.

The programmatic ad supply chain has been notoriously fragmented and non-transparent. Of the \$88 billion spent on programmatic ads, **\$22 billion is wasteful or unproductive**, according to a 2023 **study by the Association of National Advertisers**. The study closely tracked the flow of dollars through the programmatic supply chain and found that only \$0.36 of every dollar that enters a demand-side platform (DSP) reaches a consumer.

Data from these campaigns can be just as opaque. There's a lack of uniformity in how different platforms format data, which creates inconsistencies and makes it more difficult for advertisers to analyze performance.

Focusing on first-party data collection brings more transparency to digital advertising, and gives users more control over how their data is collected and shared. This is a step in the right direction: programmatic advertising (that has traditionally been steeped in third-party cookies) has felt more like surveillance than personalization to many users recently. This has resulted in people installing ad blockers, and ignoring campaigns entirely.

Publishers received approximately half of advertiser spend in the ISBA Programmatic Supply Chain Study



Developing strong relationships with customers has always been critical for brands to build a successful business, and this becomes even more vital in a privacy-first world. We will continue to support first party relationships on our ad platforms for partners, in which they have direct connections with their own customers. And we'll deepen our support for solutions that build on these direct relationships between consumers and the brands and publishers they engage with.

David Temkin,
Director of Product Management Ads, Privacy and Trust at Google
[Source](#)



Ad Tech players

Third-party cookies have been instrumental to Ad Tech players in two ways:

- Ad targeting on the open network (outside of closed systems like Google, YouTube, Facebook, etc.)
- Advertising attribution

As we know, third-party cookies have been able to track individuals from site to site, which has given an explosive number of vendors the opportunity to provide advertisers with retargeting services based on traditional cookie-based identifiers.

Without cookies, the value of cookie-based identifiers degrades significantly. However, many ad networks have been preparing for the post-cookie transition for a while now.

One initiative that's being spearheaded by The Trade Desk is Unified ID 2.0, an open-source industry initiative to achieve identity resolution across the open web. With several partners on board, including LiveRamp, Criteo, and Nielsen, Unified ID 2.0 aims to bring addressability in the open network without cookies.

The absence of third-party cookies also means that ad networks and advertisers need to rethink their attribution models, and how to instrument their analytics stack to effectively measure the customer journey and maintain accurate reporting.



It's no secret that some of the ways advertising programs work have been borderline creepy. Having a conversation over dinner about a new TV when your smartphone is 10 feet away, and then logging into your preferred online news site or social network and seeing a TV advertisement has become normal. Consumers are now pushing back, and they are more aware of alternative tools they can use for more privacy. So, instead of secretly monitoring or listening to consumer activities, publishers and advertisers must provide their target audiences with more meaningful and relevant content.

Omer Minkara,
VP & Principal Analyst, Aberdeen



As an industry, we have always put consumers front and center, innovating to meet them where they are and where they want to interact. That will not change with the erosion of third-party cookies. In fact, it will provide consumers with an additional level of control. Moving forward, access to first-party data will be critical for marketers to continue to reach these consumers in a privacy-friendly way while providing a valuable and personalized experience.

Rory Mitchell,
Executive Managing Director, Americas, at Criteo



It's hard to overstate the magnitude of what's coming: if you run mobile ad campaigns and haven't taken some basic steps before it gets here, your mobile marketing stack is about to blow up. Few ad networks and advertisers have taken the steps needed to leverage Apple's **SKAdNetwork. Without this, they remain completely reliant on traditional methods of attribution, which iOS 14 makes virtually impossible. For mobile measurement partners (MMPs) like Branch, we find that as basic app installs and ad attribution become more commoditized, it's more important than ever before to create incredible user experiences organically.**

Alex Bauer,
Head of Product Marketing at Branch



THE DIFFERENT TYPES OF DATA

03



There's a lot of uncertainty among advertisers about what a "cookie-less" world will look like. And while browser updates and privacy changes are still evolving, the one thing we do know – without question – is that first-party data is your best investment.

Think of the companies that deliver top-notch customer experiences. How does Amazon know exactly what products to recommend so you click 'add to cart'? How does Netflix keep you watching for hours? It comes down to first-party data.

This is why businesses have been shifting away from **Data Management Platforms (DMPs) toward CDPs**. While both platforms are used to build audiences for marketers, CDPs have the advantage of relying on first-party data while DMPs typically use second- and third-party data.

We'll dive deeper into the differences between a CDP and DMP below, but first, it's helpful to have a clear understanding of how first-, second-, third-, and zero-party data differ.



ZERO, FIRST, SECOND, AND THIRD-PARTY DATA


04



Zero-party data

Similar to first-party data, **zero-party data** is data a customer voluntarily shares with a business (e.g., creating an account or completing a quiz). Zero-party data provides a high level of accuracy and reliability, especially when combined with first-party data insights. For example, a customer fills out a survey with their personal preferences that a business can use to better understand their needs and create more effective marketing campaigns.



 **Registration**

Name

David Kim

Email

dkim@email.com

Address

LosAngeles,CA

Dateofbirth

Feb

▼

20

▼

1995

▼

Sign up

18

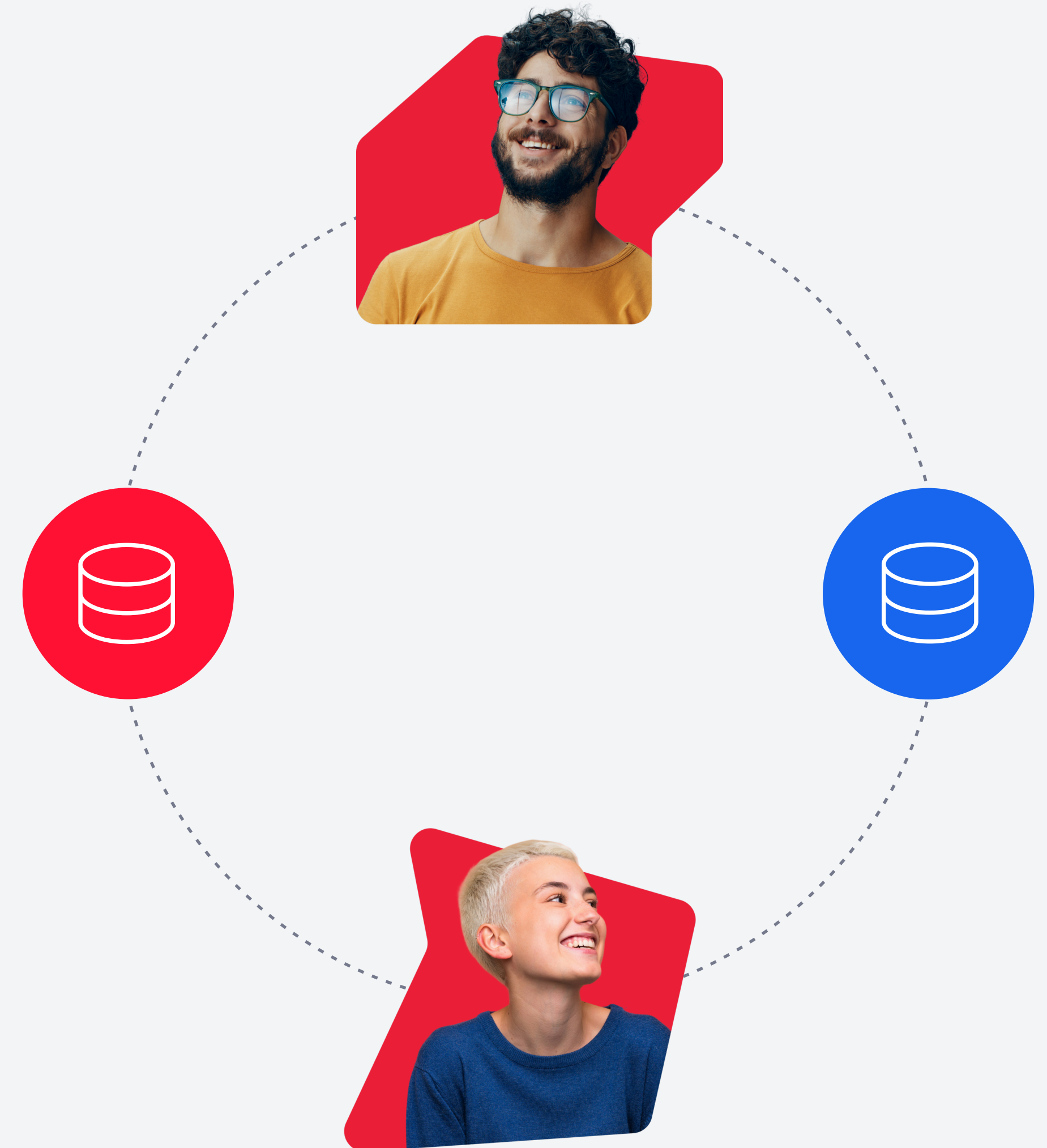
First-party data

This data is collected directly by your company (e.g., gathering an email address from a user that subscribed to your newsletter). It's generally seen as the most valuable data for understanding the customer experience, and the safest to collect. You can prove exactly where it came from and why it was collected.



Second-party data

This is first-party data collected by another company and shared with, or sold to, a non-competitive partner (e.g., partnering with a company to create an ebook, and then sharing email lists for distribution). Since this type of data comes from a partner, it's not as high quality or as safe as first-party data. For example, you attend a soccer match where your home team is sponsored by Adidas, and the next day you receive an advertisement for Adidas gear.



Third-party data

This is data that's collected by a data-collection company and then shared with anyone who wants to purchase it. Data-collection companies typically don't verify, or even guarantee, its accuracy. But in a best-case scenario, let's say you're browsing an electronics store's website for a new Mac laptop but you get distracted and start scrolling through a news website and see an ad for the same Mac.

On top of that, it's hard to prove that this data was collected ethically. Also, the fact that third-party data is available to anyone makes it less valuable: You and your competitors could be using the exact same third-party data to run your marketing campaigns.



More privacy for consumers means marketers will need to unlock the power of their first-party data to stay ahead. Building trust and delivering better experiences, powered by data, will give smart marketers a competitive advantage.

Nirish Parsad,
Marketing Technologist, Tinuiti



CPDS VS. DMPS

05



Data Management Platforms (DMPs) help advertisers manage anonymous cookie IDs for their site visitors and create audience segments for online advertising. They also provide third-party insights for these audiences via large, anonymized data sets.

DMPs get their data either by purchasing it from a data seller, or by having such a large number of clients that the DMP can aggregate and anonymize its own data.

Here's how it works: DMPs use third-party cookies (created by an external domain) on all the websites in its service. When a user clicks on an advertisement, the cookie is loaded onto their computer, and then tracks their behavior across sites. The customer could visit 50 sites, with each dropping cookies to collect the browser ID, device ID, IP address, etc., so that the DMP can recognize a specific individual (even if they remain anonymous).

So, what will happen when third-party cookies are blocked?



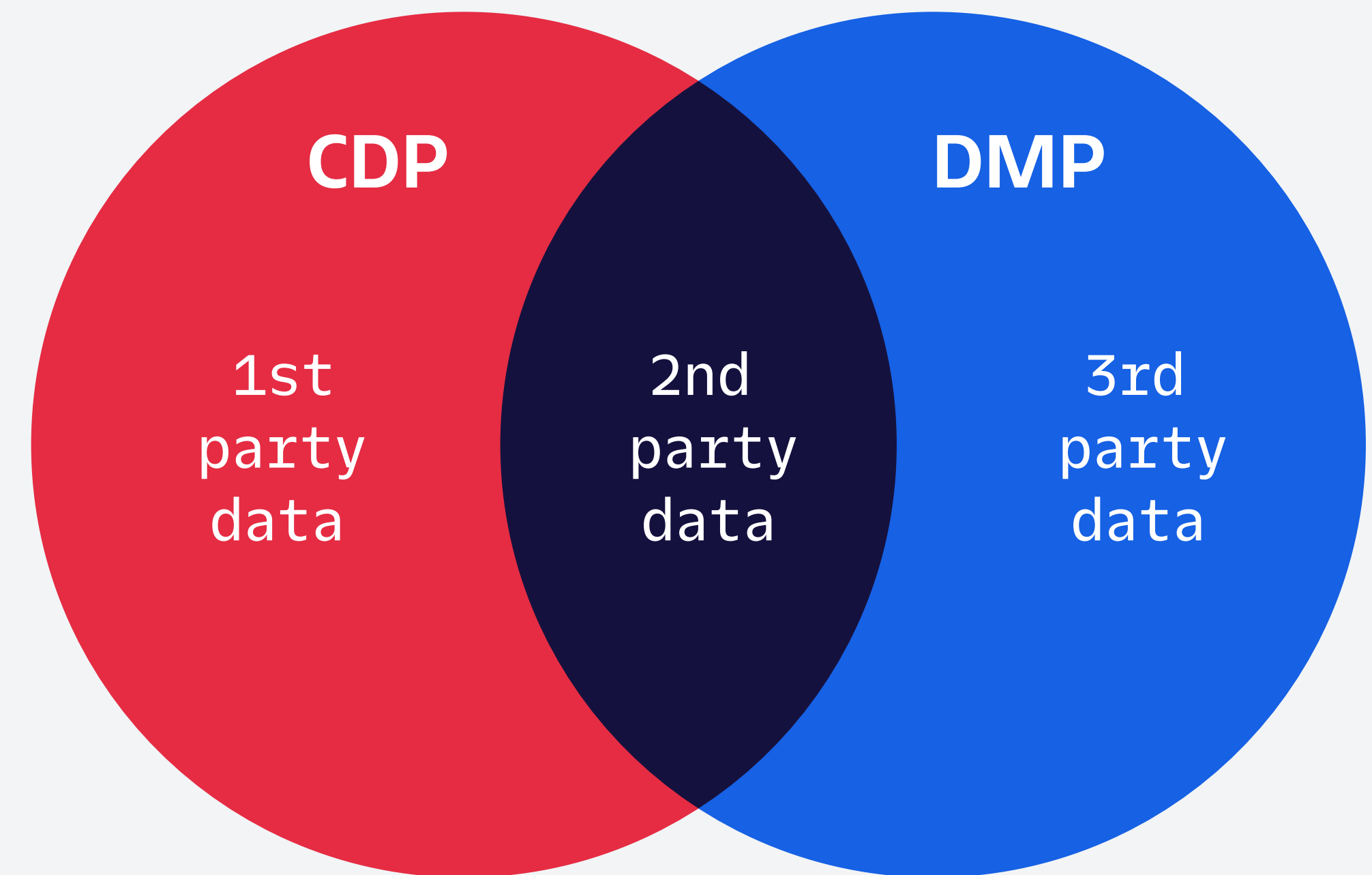
First, this type of user-specific, cross-site tracking will stop. While users can, theoretically, opt in to allow third-party cookies on their browsers, we wouldn't bet on it. This means that DMPs will only have access to previously collected user data. Audiences won't be updated, and new users will not be tracked.

CDPs, on the other hand, collect and organize first-party data from cookies that customers share directly with a brand to create a holistic, consented view of their customers. A CDP can then take that data and share it with other tools within the company's tech stack to deliver customer-first experiences.

By making the shift from DMPs to CDPs, brands can activate on a reliable single view of the customer without the need for cookie tracking or other nefarious third-party data. Customer data platforms, like [Twilio Segment](#), bring together clean, consented customer data for real-time insights so you can know each individual like they're your only customer.

Without first-party identity resolution, businesses wouldn't be able to recognize duplicate profiles on their properties, understand the full context of user journeys, or achieve reliable personalization.

(You can learn more about the nuts and bolts of identity resolution [here](#).)



Publishers and advertisers should only collect the types of data needed from consumers to engage them in a meaningful manner. Providing consumers with a simple and clear understanding of the types of first-party data the company collects, and how it's beneficial for the consumer, is a good starting point to establish greater transparency and trust between the brand and consumers.

Omer Minkara,
VP & Principal Analyst, Aberdeen



THE BENEFITS OF FIRST-PARTY DATA FOR ADVERTISERS

06



Improved accuracy

First-party data is typically more accurate than third-party data, because it reflects actual customer behavior from your own channels (web, mobile, in-store, etc.). This data begins and ends with your business; it's not filtered through some kind of intermediary or agency, as is the case with second- and third-party data.

A Think With Google and Boston Consulting Group study found that brands using first-party data for marketing have achieved a 2.9X revenue lift and a 1.5X increase in cost savings.

First-party data

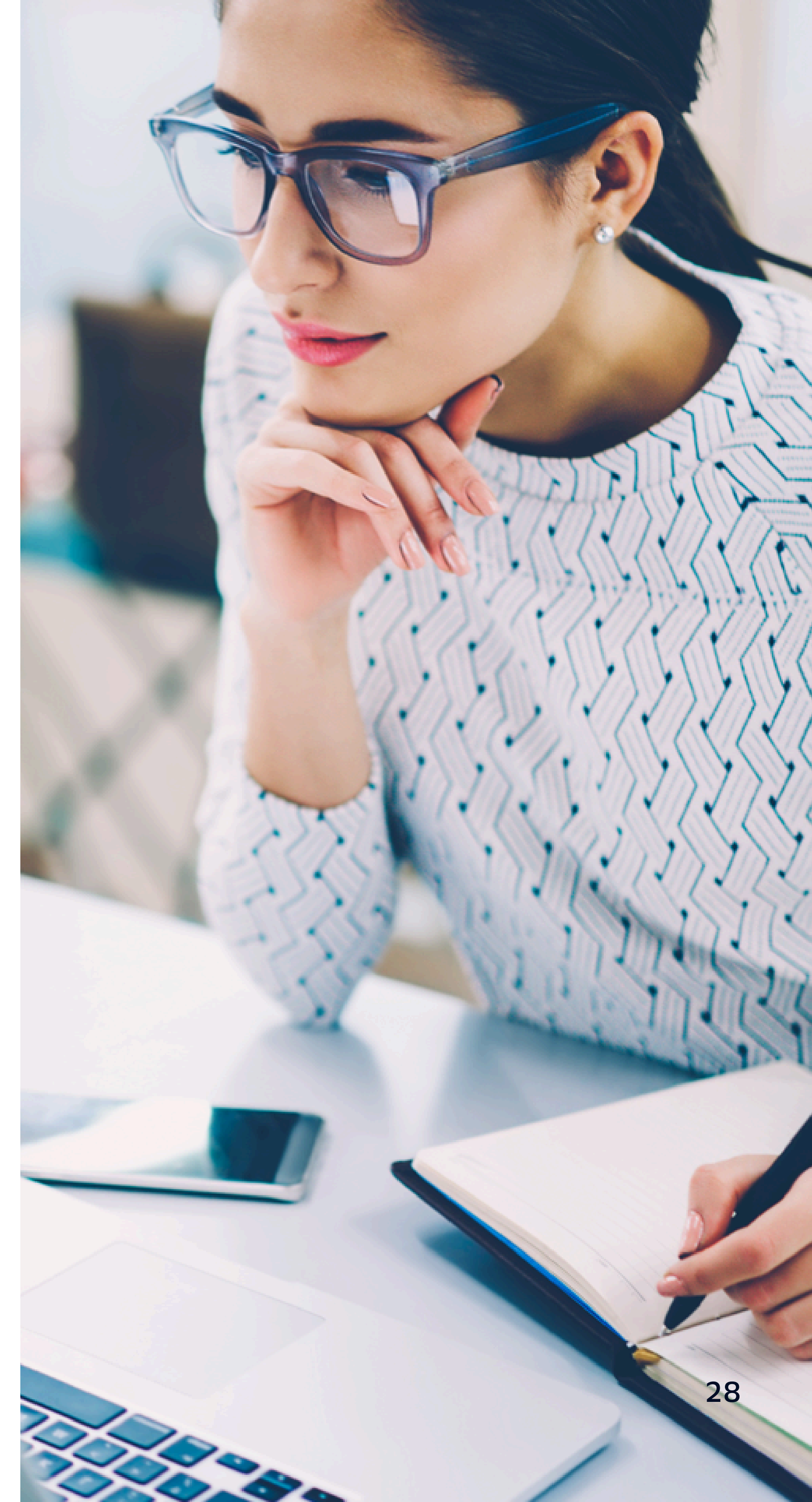
- Direct customer relationship
- Individual insights
- Collected with consent
- High accuracy

Third-party data

- Indirect customer relationship
- Aggregated insights
- Not typically collected with consent
- Low accuracy

On trend with eliminating third-party data practices is the increased focus on tracking users via server-side (instead of relying on client-side pixels on business websites).

Server-to-server tracking gives brands complete control over the data they share with advertising platforms. It's also a more accurate method of data collection: with ad blockers and browser crashes, pixels aren't always reliable at catching every user event.



At Redbubble, we've gotten ahead of the changes in third-party tracking by leveraging first-party data and server-side tracking methods to enrich our understanding of our customers in a responsible way. It's comforting to know that we are better prepared for the coming changes, and it wouldn't have been possible without Segment.

Chelsea McClure,
Director of Engagement Marketing, Redbubble



Improved ROAS

Many see the end of third-party cookies as ushering in a personalization-privacy paradox. How are businesses supposed to deliver relevant experiences without the behavioral data of third-party cookies?

But here's the thing: this "personalization paradox" doesn't exist. First-party data can power highly personalized customer experiences, while also acting as a unique differentiator: no other business has access to this data.

This not only gives businesses complete control over their data, but it establishes a more trusting and transparent relationship with customers. For advertisers specifically, you can leverage your first-party data to retarget known customers, or even power more efficient lookalike targeting in platforms like Google, Facebook, Snapchat, or Pinterest.

Without an integrated CDP, marketers have had to manually upload a CSV of their customers into advertising platforms when creating lookalike audiences. This means, from the gate, they're using outdated data. But a CDP can automate audience creation and synchronization to help businesses understand and target users in real time. (Here's a [step-by-step guide](#) on how to create lookalike audiences in Facebook using Twilio Engage, to increase advertising efficiency.)



Having Segment has not only helped us to do the personalization work we've always wanted to do, but we can now improve on the effectiveness of our ad campaigns and feed into that feedback loop.

Christian Rocha Castillo,
Deputy Director Ecommerce/Digital Media, Domino's Pizza



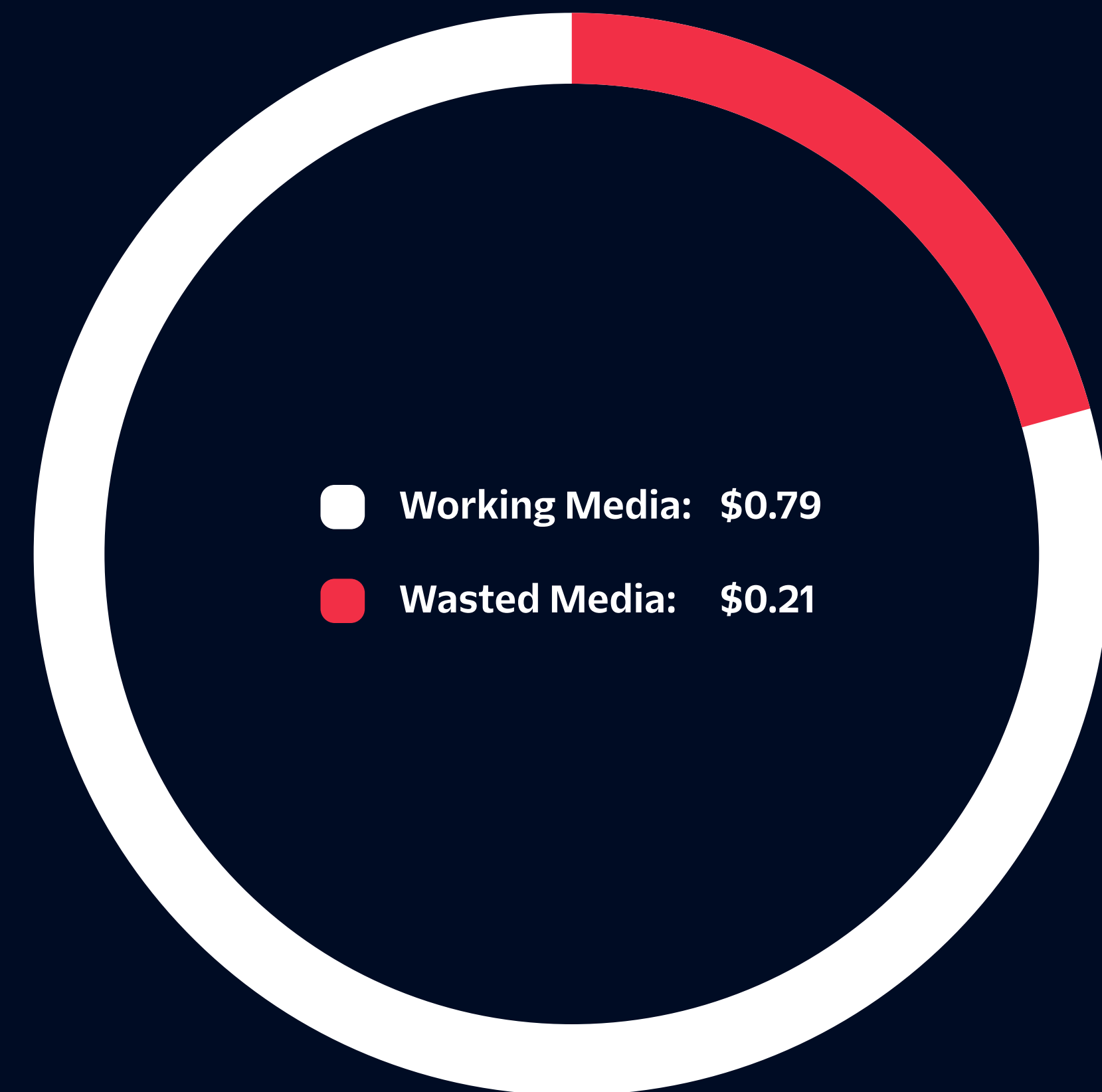
Complete view of customer activity across channels

Many marketers don't have the data infrastructure in place to work with a complete view of the customer. Instead, they have to rely on a partial view, based on breadcrumbs collected from disconnected interactions.

They don't know that Device ID 6954 is already a customer, or that Desktop User X is actually the same person as Mobile User Y. The result? Untargeted, poor performing advertising that eats up your valuable marketing budget. In fact, 21 cents of every dollar spent on advertising is wasted due to poor data quality.

A customer data platform, like [Twilio Segment](#), turns your first-party data into experiences that grow revenue by enriching customer profiles, activating customer data, optimizing ad spend, and boosting cross-sell and upsell opportunities.

Data quality impact on media effectiveness



Source: Marketing Evolution online survey conducted by Forrester Consulting. Base = 409 respondents

The ability to monitor customer journeys through connected views of first-party data will help brands understand which activities produce more desirable business results so the company can repeat them, while also enabling pivots for activities that are associated with sub-par performance results.

Omer Minkara,
VP & Principal Analyst, Aberdeen



WHY CDPS ARE PIVOTAL IN A PRIVACY- FIRST WORLD

07



The pivot to “privacy-first” digital advertising has been a long time coming. But recently it’s gained momentum.

Virginia signed consumer privacy legislation that follows in the footsteps of the California Consumer Privacy Act (CCPA) and the European Union’s General Data Protection Regulation (GDPR) – which allows users to request the deletion of their personal data collected by businesses (among other privacy measures).

CDPs have become pivotal for businesses to adapt to these regulations and stay compliant. This goes beyond first-party data collection to include data management: like the ability to [delete](#) and suppress end user data (should they request this) and [store data](#) in accordance with regional privacy laws.

Twilio Segment has championed first-party data from the start, and is in support of these privacy initiatives.

In fact, to help companies reduce long-term data exposure and easily route events to regional infrastructure, Segment has introduced Local Data Ingestion and Local Data Storage in the US and EU.

We take a proactive approach to privacy. Twilio Segment’s [Privacy Portal](#) provides real-time visibility into what personal information you’re collecting, where you’re collecting it from, and where you’re sending it, so you can set rules to automatically protect it.



We've also re-engineered the library that started it all: analytics.js. Our [latest version](#) upgrades our most popular and beloved API to offer developers more control over their first-party data collection, including adding privacy and consent controls before an event occurs.

And Twilio Segment's [Profile API](#) allows businesses to retrieve unified customer profiles in real time. These profiles, built from data collected across various touchpoints, can include predictive attributes like a customer's likelihood to churn or their predicted lifetime value. This data can be used to personalize experiences across channels and to create more precise, predictive audiences for advertising campaigns. Users can also define a target audience to be synced with advertising platforms like Facebook or LinkedIn to create lookalike audiences.

To learn more about Twilio Segment's capabilities with first-party data collection, and how it can help future-proof your digital strategy, [schedule a demo today](#).



About Twilio Segment

Companies look to a CDP – a centralized tool that helps modern businesses collect, govern, synthesize, and activate customer data.

Twilio Segment is the leading CDP with more than 450 pre-built integrations to different data sources and destinations. It provides a complete solution that eliminates the need for manual data cleansing, complex data engineering processes, and analytics reporting functions. By automating all of the backend customer data operations, Twilio Segment puts companies in a position to get the most out of their first-party data and retain customers at a higher rate.

As consumer sentiment, industry trends, and regulatory enforcement push companies away from depending on third-party data, the need for an alternative source of customer data cannot be understated. First-party data is the solution, bringing a competitive advantage as it fills the gaps where third-party data falls short: accuracy, relevance, and building customer trust.

Schedule a demo to learn how to get the most out of your customer data with Twilio Segment.



Recommended Reading



Understanding the Shift from DMPs to CDPs in the Cookieless World

This guide serves as your roadmap to exploring the limitations of DMPs, the strengths of CDPs, and equipping you with the knowledge to conquer the new data frontier.

[Download the guide](#)
>



7 Ways to Prepare for a Cookieless World

This guide explores 7 ways to pivot from third-party cookies to higher quality, first-party data, which enables businesses to offer more personalized customer experiences.

[Download the guide](#)
>



The Ultimate Guide to Customer Retention for 2024

This guide explains the importance of customer retention as a strategy to reduce customer acquisition costs as well as to increase customer loyalty and LTV.

[Download the guide](#)
>



All rights reserved. Copyright @ 2025 Twilio Inc.