



CLEARCODE

The AdTech Book

The platforms, processes, and players that make up the digital advertising industry

From the first-ever ad servers, to real-time bidding (RTB), through to header bidding. The AdTech Book provides a detailed overview of the entire digital advertising industry from the very beginning right through to today.

Whether you work in online advertising, build advertising technology, or simply want to learn more about the engines that power the Internet, The AdTech Book provides you with the answers to all the questions that you've ever had about online advertising.

Here's a brief overview of what you'll learn by reading this book:

- **Discover** the history behind the digital advertising industry and how it has evolved over the past 20+ years.
- **Learn** about the role each technological platform plays in the digital ecosystem and how they work.
- **Understand** how the various processes work behind the scenes to serve ads to online visitors.
- **Identify** the role data plays in online advertising, including how it is collected and utilized by advertisers and publishers.
- **Learn** about the terminology and acronyms used in digital advertising.
- **Educate** yourself about the challenges facing the digital advertising ecosystem, including ad fraud, ad blockers, ad viewability, and transparency.
- **See** the online advertising industry from the consumer's perspective and how it powers the Internet.

About the Authors

[Clearcode](#) is a full-service AdTech and MarTech development company, led by [Piotr Banaszczyk](#), CEO, and [Tomasz Chmielewski](#), COO. You can learn more about Clearcode [here](#).

The AdTech Book has been contributed to and written by various team members of [Clearcode](#), with the main contributors being [Maciej Zawadziński](#), Clearcode's co-founder and CEO of [Piwik PRO](#), and [Michael Sweeney](#), Head of Marketing at Clearcode.

This book is the result of Clearcode's many years of experience in designing, developing, launching, and maintaining advertising and marketing technologies for our clients.

Table Of Contents

[01. Introduction](#)

[02. Advertising basics](#)

[The Advertiser-Publisher Relationship](#)

[What is an Advertiser?](#)

[Why Do Brands and Companies Advertise?](#)

[What is a Publisher?](#)

[What is Advertising Technology \(AdTech\)?](#)

[Important Terms Explained](#)

[Chapter Conclusion](#)

[03. The History of Online Advertising Technology](#)

[Advertising Moves Online](#)

[04. The Main Technology Platforms and Intermediaries in the Online Display Advertising Ecosystem](#)

[Advertisers – The Buy Side](#)

[Intermediaries](#)

[The Sell Side \(Publisher\)](#)

[How AdTech Companies Make Money](#)

[The Walled Gardens](#)

[Standardization in the Ecosystem](#)

[05. The Main Digital Advertising Mediums and Channels](#)

[Advertising Mediums](#)

[Advertising Channels](#)

[06. Ad Serving](#)

[What Is an Ad Server?](#)

[Campaign Execution Using an Ad Server: Then and Now](#)

[How Does an Ad Server Work?](#)

[First-Party vs. Third-Party Ad Servers: A Simple Comparison](#)

[Technical Zone](#)

[How Ad Serving Works From a Technical Perspective](#)

[The Anatomy of an Ad Server](#)

[Chapter Summary](#)

[07. Ad Targeting and Budget Control](#)

[Contextual Targeting](#)

[Keywords](#)

[Ad Slot and Ad Position](#)

[Publisher's URL](#)

[Domain](#)

[Section and URLs](#)

[IP and Geolocation](#)

[Browser Type, Operating System and Device Type](#)

[IAB Content Taxonomy](#)

[Day of Week and Time of Day](#)

[Behavioral Targeting](#)

[Retargeting](#)

[Demographic](#)

[Controlling a Campaign's Budget](#)

[Chapter Summary](#)

[08. Tracking and Reporting Impressions, Clicks, and Conversions in AdTech Platforms](#)

[Impression, Click, and Conversion Tracking](#)

[Reporting](#)

[Chapter Summary](#)

[09. Media-Buying Methods: Programmatic, Real-Time Bidding \(RTB\), Header Bidding, and PMP](#)

[The Main Media-Buying Processes](#)

[Manual Media Buying](#)

[Programmatic Media Buying](#)

[Programmatic Direct](#)

[Real-Time Bidding \(RTB\)](#)

[How Does RTB Work?](#)

[Private Marketplace \(PMP\)](#)

[A Comparison Table of the Above Media-Buying Processes](#)

[The Publisher's Waterfall](#)

[Header Bidding](#)

[Waterfall vs. Header Bidding: Benefits and Drawbacks](#)

[Auction Dynamics: First- and Second-Price Auctions and Hard and Soft Floor Prices](#)

[Second-Price Auctions \(2PA\)](#)

[First-Price Auctions \(1PA\)](#)

[Chapter Summary](#)

[10. User Identification](#)

[Why Do We Need to Identify Users?](#)

[Different User-Identification Methods](#)

[Web Browsers](#)

[Cookies](#)

[Device Fingerprinting](#)

[HTML5 Local Storage](#)

[ETags](#)

[Evercookies](#)

[How Different Web Browsers Handle Cookies, Device Fingerprints and Local Storage](#)

[Mobile Devices](#)

[Mobile Web Browsers](#)

[Mobile Apps \(In-App\)](#)

[Cookies](#)
[Advertising IDs](#)
[Open Device Identification Number \(ODIN\)](#)

[User Profile Matching](#)

[Deterministic and Probabilistic Matching](#)
[What Are Deterministic and Probabilistic Matching Used For?](#)

[The Main Challenges With Identifying Users on Web Browser and Mobile Apps](#)

[Solutions to the Identity Problem](#)

[How Do These ID Solutions Work?](#)
[ID and Device Graphs](#)
[How Do ID Graphs Work?](#)
[The Challenges Facing These ID Solutions](#)

[The Future of User Identification in Web Browsers and Mobile Apps](#)

11. Data Management Platforms (DMPs) & Data Usage

[The Different Types Of Data: First-Party, Second-Party, And Third-Party Data](#)

[First-Party Data](#)
[Second-Party Data](#)
[Third-Party Data](#)
[A Comparison Of The Value Of First-, Second-, And Third-Party Data](#)

[Where Is Data Obtained?](#)

[Online Sources](#)
[Offline Sources](#)
[Combining Online and Offline Data Together](#)

[The Data Fragmentation Problem](#)

[Data Management Platform \(DMP\)](#)

[Data Collection in a DMP](#)

[Pixels and Tags](#)
[Piggybacking](#)
[Tags](#)
[Application Program Interface \(API\)](#)
[First-Party Data Onboarding](#)

[Data Normalization and Enrichment in a DMP](#)

[Profile Building and Merging](#)

[Data Storage](#)
[Data Taxonomies](#)

[Audience Segmentation and Creation](#)

[How A DMP Creates Audience Segments](#)

[Use Cases Of Data Activation With A Data Management Platform \(DMP\)](#)

[Data Activation for Advertisers](#)
[Data Activation For Publishers](#)
[Data Brokers and Integrations With Programmatic Media-Buying Platforms](#)

[The Future of DMPs](#)

[What Is a Customer Data Platform \(CDP\)?](#)

12. Attribution

[What Is Attribution?](#)

[Online to Online Attribution Models](#)

[How Does Online Attribution work?](#)

[Online Attribution Models](#)

[Cross-Device Attribution](#)

[How Does Cross-Device Attribution Work?](#)

[Offline-Online Attribution](#)

[Online-Offline Attribution](#)

[The Multi-Device Consumer Journey And The Technological Challenges It Presents](#)

13. Ad Fraud and Viewability

[Ad Fraud](#)

[The Cost of Ad Fraud](#)

[The Main Types of Ad Fraud](#)

[How Ad Fraud Is Carried Out](#)

[Ad Fraud in Emerging Areas of Digital Advertising](#)

[How Advertisers And Publishers Can Defend Against Ad Fraud](#)

[Ad Viewability](#)

[Viewable Impressions](#)

[Chapter Summary](#)

14. User Privacy in Digital Advertising

[The Rise of Consumer Data Collection and Privacy Concerns](#)

[Privacy and Data Protection Laws Around The World](#)

[The European Union's General Data Protection Regulation \(GDPR\)](#)

[The European Union's ePrivacy Directive](#)

[California Consumer Privacy Act of 2018](#)

[CCPA vs GDPR: What Are the Similarities and Differences?](#)

[The Definition of Personally Identifiable Information \(PII\) and Personal Data](#)

[The Definition of Personal Data](#)

[Browser Settings](#)

[Apple's Safari](#)

[How Does Intelligent Tracking Prevention Impact Digital Advertising?](#)

[Privacy Changes in iCloud+](#)

[Mozilla's Firefox](#)

[Google Chrome](#)

[Chrome's Better Ads Standards](#)

[Chrome's SameSite Cookies](#)

[Chrome's Privacy Sandbox](#)

[Chrome's Plans to Kill Off Third-Party Cookies and the Move To Privacy Sandbox](#)

[Mobile IDs](#)

[Apple's AppTrackingTransparency \(ATT\) Framework](#)

[Apple's SKAdNetwork](#)

[Apple's Privacy Changes in iOS 15 and iPad 15](#)

[Google's Android Advertising ID \(AAID\)](#)

[Ad Blockers](#)

[How Do Ad Blockers Work?](#)

[The Impact Ad Blockers Have On The Digital Advertising Industry](#)

[What Can Publishers Do About Ad Blockers?](#)

[How can publishers detect if someone is using an ad blocker?](#)

[How can publishers deal with ad blockers?](#)

[Opting Out Of Online Behavioral Advertising](#)

[How can Internet users opt-out of behavioral or targeted online advertising?](#)

[The Implications Of Opt-Out Solutions](#)

[Differing Views on Data Collection](#)

[Online Ads And Their Common Pitfalls Of The User Experience](#)

[The Future of User Privacy in Digital Advertising](#)

[15. AdTech From The Vendors' And Agencies' Perspective](#)

[AdTech from the Vendor's Perspective](#)

[AdTech Business Models](#)

[The Main Technical Challenges of Running an AdTech Company](#)

[AdTech from the Advertising Agencies's Perspective](#)

[In-House Programmatic Vs In-House AdTech](#)

[1. The Traditional Way of Buying Digital Media](#)

[2. An Ad Agency Takes Programmatic Buying and AdTech In-House](#)

[3. A Brand Takes Programmatic Buying In-House](#)

[4. A Brand Takes Programmatic Buying and AdTech In-House](#)

[Advertising Technology: The Build vs Rent Dilemma](#)

[Build vs Rent: From The Business Perspective](#)

[From The Technology Perspective](#)

[16. Programmatic & AdTech in 2022: Challenges and Opportunities](#)

01. Introduction



If you were to peel back the curtains on the ads you see on websites and mobile apps, you would be amazed at what's happening behind the scenes. The online advertising ecosystem consists of companies, technology systems, and complex technical processes all working together to serve ads to online users across the Internet.

Online advertising has brought with it a number of positives. For one, it's provided content creators with a source of revenue so they can distribute their content for free to online users. It's also allowed new and existing media and technology businesses to grow and thrive.

However, while the online advertising industry has experienced a number of ups, there have also been many downs. Some key examples include being hit hard by the dot-com bubble in the late 1990s/early 2000s, and more recently, the introduction of privacy laws (e.g. the GDPR) and privacy settings in browsers (e.g. Safari's Intelligent Track Prevention) that have negatively impacted advertisers, AdTech companies, and publishers.

Why Have We Written This Book?

Throughout our 12+ years of designing and building advertising and marketing technology, we've noticed 2 things:

1. The platforms and processes that make up AdTech are highly complex.
2. There are very few resources out there that explain in an easy-to-understand and transparent way how online advertising works from both a fundamental and technical perspective.

It came to our attention that we were essentially sitting on a gold mine of knowledge that we could share with others.

And thus the idea of **The AdTech Book** was created.

Who Is The AdTech Bible Written For?

The AdTech Book is ideal for anyone wanting to learn about the history of online advertising and understand how the different elements of the digital advertising technology ecosystem work, what their roles are, and the relationships between different parties in the industry.

Even though the book contains a lot of highly technical and detailed explanations, we've tried to write the AdTech Book in the most straightforward way possible so that anyone can read and understand the contents of the book.

More specifically, the book will greatly benefit:

- C-level executives and founders at advertising and marketing companies.
- Advertisers and marketers who work in-house or at advertising and digital agencies.
- Programmers and technical teams that build advertising and marketing technology.
- Publishers and content creators who monetize (or want to) their content with advertising.
- Regular, everyday web surfers who want to learn how online advertising works.

General Assumptions

This book assumes that you grasp the concept of how ads are used to monetize websites and promote products and services. This book does not assume that you have any kind of technical knowledge of how the platforms and processes work, however if you do, then you will find that it is a lot easier to understand the technical explanations covered throughout the book.

How This Book Is Organized

The first few chapters of the book introduce the history of online advertising and set the scene for the subsequent chapters. We cover the fundamentals of digital advertising and then slowly start to introduce the platforms, intermediaries, and technical processes.

Conventions Used In This Book

Bold

Highlights certain terms.

Brand awareness (aka branding): The main goal is to reach a broad consumer audience, engage with them, and maximize the time they are exposed to the brand.

Italics

Used to highlight a specific term in a sentence, e.g:

A publisher can be defined as any company that produces content that attracts an audience.

Bold and italics

Indicates new terms, e.g:

Advertising Technology (Ad Tech, AdTech, adtech, ad tech, ad technology) refers to the software and tools used to create, run, manage, measure, and optimize online media campaigns.

Italics, underline and bold

Used when referring to chapters for further reading, e.g:

See the chapter **The Main Digital Advertising Mediums and Channels** for more information about the different types of digital advertisements.

The Light Grey Boxes

Throughout this book, you'll see light grey boxes like this one. These boxes have 2 purposes -

1. Explain certain terms located in the surrounding text.
2. Provide interesting facts related to the topics being discussed.

Code Examples

The code examples featured in this book are used for explanation purposes only. They are not designed to be copied and used unless stated otherwise.

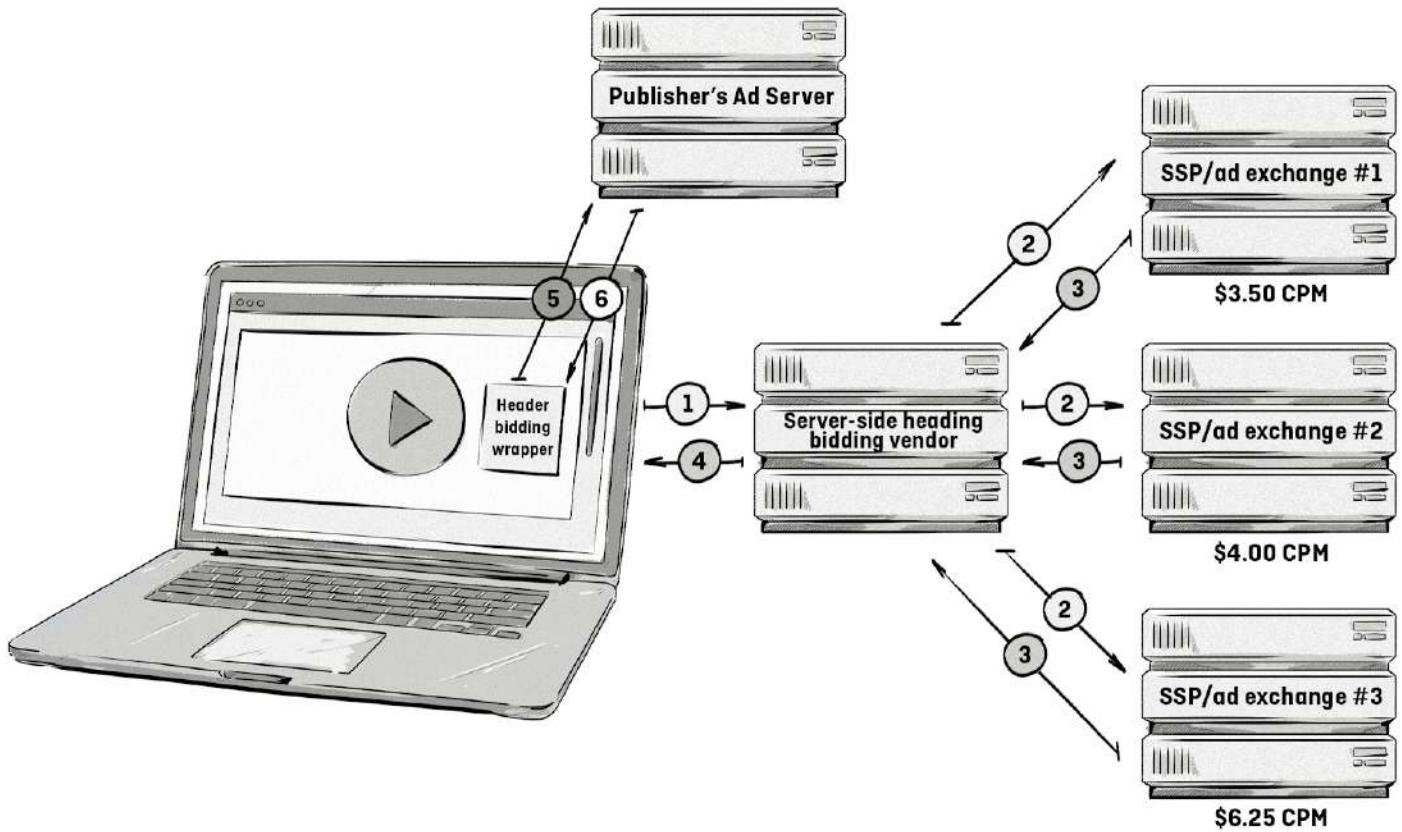
```
<a href="https://www.advertisers-landing-page.com">  </a>
```



Technical Illustrations, Explanations, And Examples

Throughout this book, whenever we illustrate, explain, or provide an example of a technical aspect (e.g. a process such as server-side video header bidding) we are doing so in the most common or straightforward way possible in order to avoid the concept being lost in a sea of confusion.

It's also worth noting that there is often more than one way to carry out the technical processes mentioned in this book.



An illustration about how server-side video header bidding works.

Terminology Used In The Book

You'll notice that in this book we refer to the same thing by different names. For example:

Inventory, also known as **ad space** or **online media**, is the available space a publisher has on its site or app.

This is common within the online advertising industry, but to avoid confusion, we will aim to only use one term throughout the book.

The only exception to this are the terms **online advertising** and **digital advertising**. Although these terms are not synonymous with one another, we'll use both terms sparingly throughout the book to refer to the same thing — advertising delivered and displayed on the Internet or digital devices.

You can view a list of popular terms in our [AdTech glossary](#).

We'd Love To Hear From You

We've written this book for you, so if there is something you think we can add or improve on, please feel free to contact us and let us know.

The contents and information in this book have undergone numerous iterations and edits, however, mistakes and oversights can occur.

If you happen to find any errors or simply want to provide feedback, then please contact us via adtechbook@clearcode.cc and we'll review and apply them to further editions.

We can also be contacted via the following channels:

Web: clearcode.cc

LinkedIn: linkedin.com/clearcode

Twitter: [@clearcodehq](https://twitter.com/clearcodehq)

Facebook: facebook.com/clearcode

02. Advertising basics



The Advertiser-Publisher Relationship

Digital advertising is a global multibillion-dollar industry comprising thousands of companies, but at the heart of it all are two key players: [the advertiser](#) and [the publisher](#).

The advertiser-publisher relationship dates back well before the invention of the internet. Publishers, such as newspapers and magazines, would sell ad space to advertisers as a way to generate additional revenue on top of their regular subscriptions and individual sales.

Nowadays anyone can become a publisher by simply creating a website or developing a mobile app and selling ad space to advertisers. This has completely changed the dynamics of the traditional advertiser-publisher relationship.

What is an Advertiser?

An **advertiser** is a brand or company (e.g. advertising agency) that wants to get its product or service in front of its target audience to build brand awareness, develop brand loyalty, and increase sales.

Below are some examples of brands that spend billions of dollars (\$USD) per year on advertising:



Procter&Gamble **verizon**  **General Motors**

Advertisers aren't only big brands, however; millions of small- and medium-sized enterprises (SMEs) and organizations advertise their services and products online every day.

Large brands, such as those listed above, are often represented by **advertising agencies**, whose job it is to:

Create the campaign: Designing the graphical elements and message of the ad.

Execute the campaign: Configuring the campaign (e.g. setting up targeting and frequency capping) and launching it across different channels (e.g. web, in-app, and DOOH).

Manage the campaign: Measuring campaign results and making changes to improve performance.

A brief history of advertising agencies

The first agencies date back as far as 1786 when William Taylor opened his office in London, today acknowledged as the first advertising agency in history.

However, while the UK business is considered the precursor of advertising agencies in Europe, it was Volney B. Palmer who took the idea across the ocean, opening the first agency on American soil in Philadelphia in 1842.

Volney would buy large amounts of space in various newspapers at a discounted rate, then resell the space at higher rates to advertisers. The actual ad, including the copy, layout, and artwork, was prepared by the client, which basically made Palmer an ad-space broker with little influence on the creative side.

Some agents, at the request of their clients, created directories with advertising rates of newspapers in New England. Many agencies made a profit buying newspaper space and reselling it with a markup.

Many other advertising agencies soon followed the same business model until the 19th century when N.W. Ayer & Son was founded in New York.

The agency, rather than simply selling space, provided a full range of services, including planning, creating, and executing complete campaigns for its customers.

It made itself famous working for clients such as De Beers, AT&T, and the U.S. Army, creating a number of memorable slogans.

We talk more about ad agencies in [Chapter 04: The Main Technology Platforms and Intermediaries in the Digital Advertising Ecosystem](#)

Source: [Adland: A Global History of Advertising](#), published by Kogan Page; Second edition (July 28, 2013)

Throughout this book, you'll see us use the term **advertiser**, which can either refer to an advertiser working in-house at a brand, or an ad agency working on behalf of a brand.

Why Do Brands and Companies Advertise?

There are a number of reasons why brands and companies advertise. Below are some of the main advertising strategies:

Brand awareness: Reach a broad consumer audience, engage with them, and maximize the time they are exposed to the brand.

Direct response (aka prospecting, acquisition): Generate new leads, sales, and conversions by displaying ads that persuade the consumer to take some sort of action, such as fill in a form.

Retention: Re-engage with existing customers and consumers who have previously interacted or been exposed to a brand, which is very often conducted via retargeting (aka remarketing) campaigns.

What is a Publisher?

A **publisher** can be defined as any company that produces content that attracts an audience.

Examples of publishers include newspapers and magazines in the offline world, and websites and mobile apps in the online world.



Above are examples of publishers displayed on different devices. Notice how they all have an ad displayed?

The term *publisher* doesn't solely refer to websites, it can also extend to content or publishing platforms, such as YouTube, Facebook, and Hulu.

How Do Publishers Monetize Their Websites and Apps?

There are a number of ways publishers can monetize their websites or apps depending on their strategy. Some monetization methods include:

Digital Ads



This is by far one of the most popular ways to monetize websites and apps of all shapes and sizes. Depending on the pricing model, publishers can either make money each time a visitor clicks on an ad or for every 1,000 impressions.

*See chapter 05. **The Main Digital Advertising Mediums and Channels** for more information about the different types of digital advertisements.*

Paywalls and Registration Walls



Many popular news and premium-content sites hide their content behind paywalls and registration walls.

Paywalls: Require users to either buy a subscription or pay a one-time fee to access the content.

News and media companies are increasingly implementing paywalls as a way to make up for the financial losses they've experienced as a result of ad blockers.

Registration walls: Require users to create a free account, or simply provide their email address in order to access the content.

Registration walls allow publishers to collect first-party data and build addressable audiences.

Publishers can then offer these audiences to advertisers, which can be used for ad targeting. However, this method is still susceptible to ad blockers.

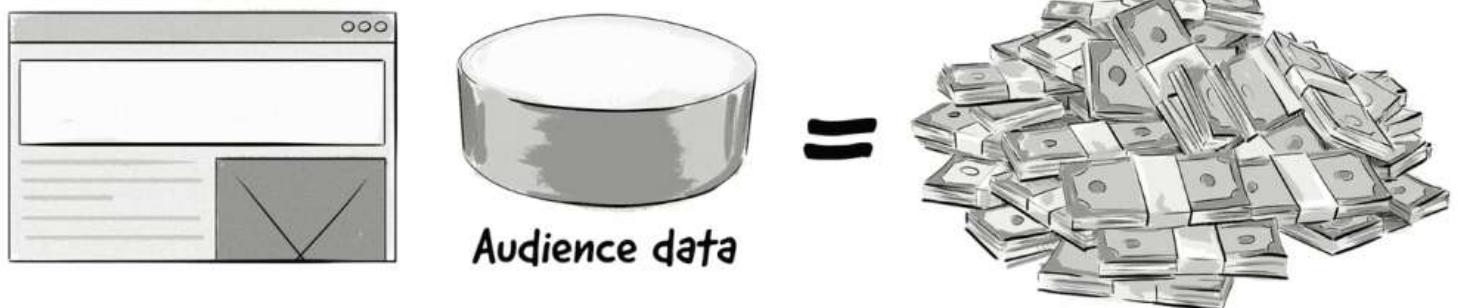
Products and Services



There are some publishers that monetize their websites by either selling their own products and services or by partnering with other companies and promoting their products and services, for which they would receive a commission or percentage of the revenue.

Examples include e-commerce stores, affiliate sites, industry-research companies, and sites that offer other premium content and digital goods.

Selling Data



Large publishers with access to thousands of data sets and user profiles are able to sell the information to data brokers or directly to advertisers.

Now that we've defined the two most important players in the online-advertising ecosystem, it's time to embark on our journey through the online-advertising world, starting with a brief introduction about the technology that powers it all.

What is Advertising Technology (AdTech)?

The way in which online advertising campaigns are run in today's digital world look completely different to how campaigns were run over the past 150+ years of advertising.

It's all thanks to the rise of advertising technology, which has transformed the way media buyers manage, measure, and optimize online advertising campaigns.

Advertising technology (also written as **Ad Tech**, **AdTech**, **adtech**, **ad tech**, **ad technology**) refers to the software and tools used to create, run, manage, measure, and optimize digital advertising campaigns.

All parties involved in digital advertising—from brands and advertisers to ad agencies, technology vendors, and publishers—use one or more pieces of advertising technology.

Since the very first pieces of AdTech were introduced in the mid-1990s, a number of new systems have emerged to solve various problems and capitalize on new opportunities that have risen along the way.

AdTech has revolutionized the way brands connect with their audiences and helped both sides get what they want and need:

Advertisers: Want successful ad campaigns targeted at highly engaged and valued audiences with measurable results.

Publishers: Want high percentages of ad inventory sold at the highest possible price with minimal overhead costs.



The Energy Drink Co.



Daily News



In the image above, the advertiser (The Energy Drink Co.) pays to have its ads displayed on the publisher's website (Daily News).

In essence, this has always been the goal of advertising, but the popularization of the Internet and introduction of AdTech added new channels, mediums, and scale, among other things, to the entire process.

For example, instead of a brand or ad agency in Chicago calling up the *Chicago Tribune* and placing an order for a full-page ad in the Sunday edition with the intention of reaching Chicagoans, the brand could now buy ad space on multiple publishers' websites and only display ads to people from Chicago that would potentially be interested in buying the advertiser's product or service.

These visitors would match the advertiser's ideal target-customer profile (aka target audience), made up of a range of criteria, such as demographics, interests, behaviors, recent purchases, and web history.

The advertiser would also want to reach its desired audience at the right time, at the right place, and on the right device—for example, during business hours at home on a laptop, or late-night in a city center on a mobile device.

We talk more about ad agencies in chapter 04: The Main Technology Platforms and Intermediaries in the Digital Advertising Ecosystem

What is a target audience?

A [target audience](#) is a group of consumers who are the best fit for potential buyers of an advertiser's product or service. They are typically characterized with certain needs or desires.

Usually, the target audience can be based on a combination of demographics, interests, and/or behaviors of the consumers.

It's not only the medium that has changed, but the actual media-buying and selling process has also adapted to the online world.

Back when brands would advertise in newspapers and magazines, the brand's advertisers would contact the newspaper's sales team directly and purchase available ad space.

Nowadays, most online media is bought and sold with the use of advertising technology, but it is responsible for more than just moving an ad from an advertiser to a publisher.

Here's a list of just some of the things AdTech is responsible for:

- Making decisions about which ads to display to a specific group of users based on the advertiser's targeting criteria.
- Delivering online media (ads) across different channels (web and in-app mobile) and devices (smartphones, laptops, tablets, etc.).
- Optimizing campaign performance for advertisers and yield for publishers.
- Collecting data about users and creating audiences.
- Producing measurement and analytics reports.
- Billing and media-buying process management.

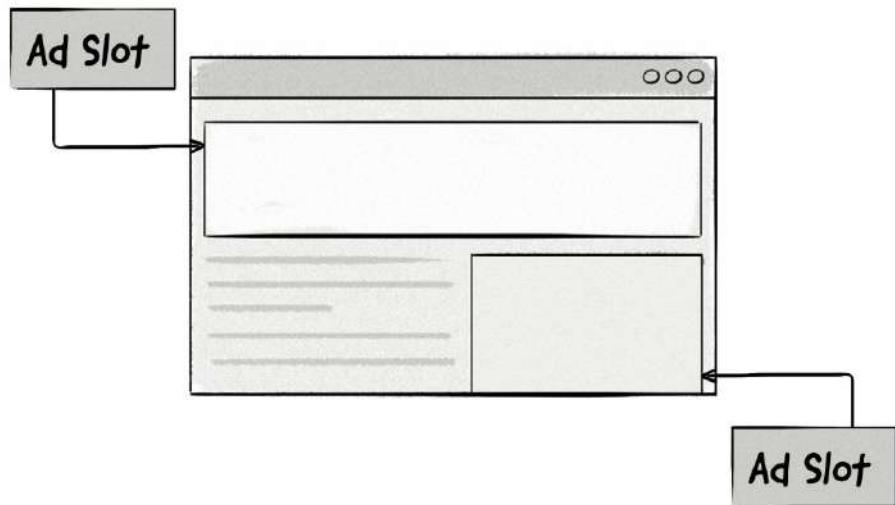
In chapter 04. The Main Technology Platforms and Intermediaries in the Online Display Advertising Ecosystem, we take a closer look at how the different AdTech platforms work and the role they play in digital advertising.

Important Terms Explained

One of the main things you'll discover by reading this book, if you haven't already, is that the online advertising industry has its own terminology and an endless supply of initialisms.

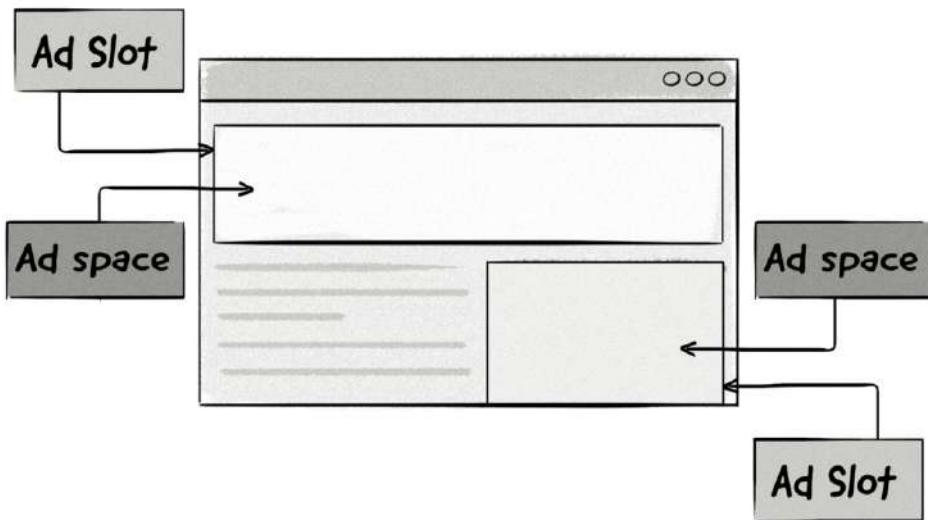
We'll now take a look at some of the most important terms that you'll come across throughout this book, but you can also check out our [AdTech Glossary](#) for an extensive list of advertising technology terminology. // We'll now take a look at some of the most important terms that you'll come across throughout this book, but you can also check out our [AdTech Glossary](#) located at the end of this book for an extensive list of advertising technology terminology.

Ad Slot



An **ad slot** refers to the actual space on a website that is filled with ads. You can think of this as a dedicated part of a website for displaying ads. In an ad slot there is an **ad tag** that communicates with the ad server to load an actual ad.

Ad Space

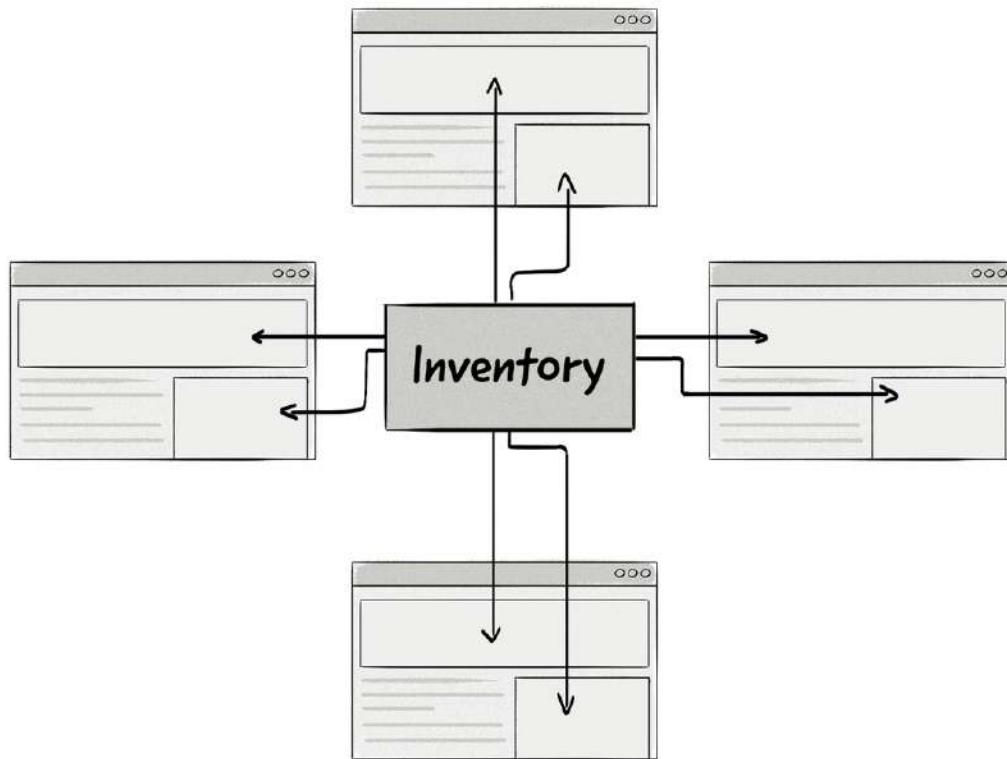


Ad space is the actual impression available in the ad slot. The terms **ad space** and **ad slot** are often used interchangeably, but the main difference is that an ad slot is where the ad space is hosted.

To help clarify this point, think about a billboard. The actual billboard would be the ad slot and the white section inside the billboard where the ads are placed would be the ad space.

Inventory

Inventory, aka **ad inventory**, is the name given to all the ad space available on a website. Sometimes, *inventory* and *ad space* are used interchangeably.



There are three main types of inventory: **premium**, **remnant**, and **long-tail**.

Premium inventory is a publisher's most sought-after or most-valuable inventory. It is often inventory located on recognizable publisher sites and typically on high-traffic pages, such as a home page, or in highly visible areas, such as at the top of a page.

Remnant inventory is inventory that a publisher has been unable to sell directly to advertisers through direct deals and other primary inventory-monetization channels. It's basically leftover inventory publishers are willing to sell for less than their standard price.

Long-tail inventory is inventory found on small sites and blogs. A large chunk of this type of inventory is sold via Google AdSense. Long-tail sites sometimes seek better monetization alternatives to AdSense, for example, by joining affiliate programs and networks.

Creative

A **creative** is the file containing the actual advertisement that the user is exposed to. The most common types of creatives are graphical files (either static or animated), video files, and audio files, and can come in many formats, including GIF, JPEG and HTML5 (earlier Flash), as well as MOV, FLV, MP4 for video files.



Examples of different types of ads.

Creative Specifications

Creative specifications prepare every party in the ecosystem to receive, handle, and display the advertisements, from ad agencies designing the creatives, to AdTech vendors delivering and measuring the ads, through to publishers preparing their sites to display ads.

These specifications have been developed by the **Interactive Advertising Bureau (IAB)**, an organization designed to deliver standardization to the online advertising industry.

For the most part, creative specifications:

- Specify dimensions, size, and file formats. For example:
 - 300x250 pixels (dimensions). Maximum 100 KB (size). HTML5, GIF, or JPEG (file format).
- Outline good practices. For example:
 - The <noscript> tag should be applied, as this provides a path to an alternate image when users have scripts disabled in their browser.
 - LEAN principles: **L**ightweight, **E**ncrypted, **A**d-choice-supported, **N**on-invasive ads.
- Define functional requirements, such as:
 - Maximum animation length of 15 seconds.
 - Audio must be user initiated (i.e. they must mute/unmute the audio), with mute being the default state.
 - Expansion is not allowed.
- Include other technical requirements. For example:

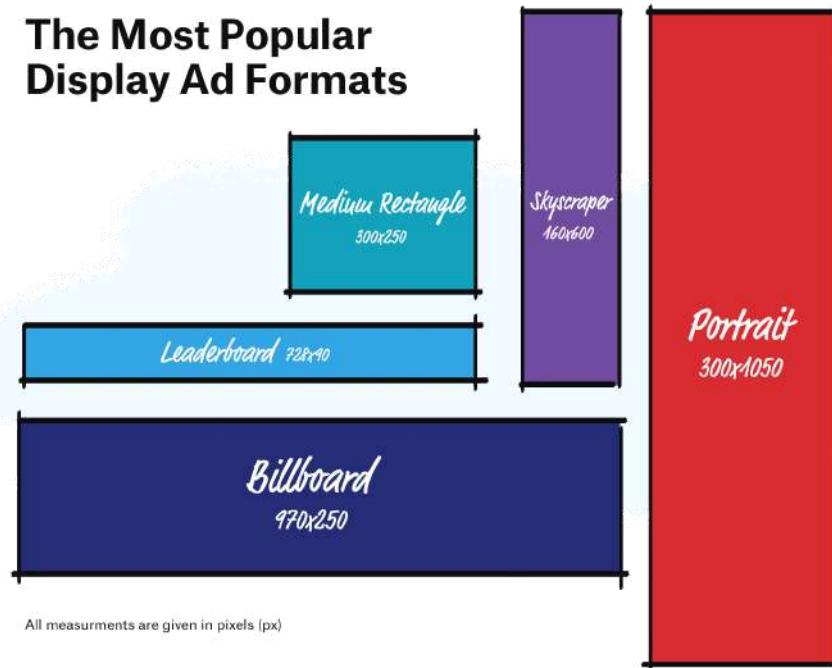
- A minimum 24 frames per second (fps).
- Z-index guidelines to specify the content elements on a webpage. These guidelines help publishers provide a seamless user experience by ensuring ads are displayed on the correct CSS layer, which prevents ads and the publisher's content (e.g. text and images) from being displayed on top of one another.

Display Ad Formats

You would have noticed already that ads shown in web browsers can come in different shapes and sizes depending on where they are shown and on which device they are displayed (e.g. desktop or mobile).

Each type of ad has its own set of formats, most of which were created by the IAB in the late 1990s/early 2000s as a way to create a standard for the industry and make it easier for advertisers and publishers to trade media.

Traditionally, the most popular online ad formats have been the following:



These types of ad formats were part of the universal ad package (UAP), which was used in online advertising for most of the past decade.

Flexible Size Ad Specifications

Ad Type	Ad unit Name	Transition Fixed Size Ad unit (px)*	Aspect Ratio (width:height)	Ad Size**	Size Range		Max. K-Weight (kB)		Static Image Size (dp)
					Min. Size Width x height (dp***)	Max. Size Width x height (dp***)	Initial Load	Subload	
Horizontal	2x1	Half Page	2:1	X Large	900x450	1800x900	250	500	1800x900
	2x1	N/A	2:1	Small	300x150	450x225	100	200	
	4x1	Billboard 970x250	4:1	X Large	900x225	1800x450	250	500	1800x450
	6x1	Smartphone Banner 300x50, 320x50	6:1	X Small	300x50	450x75	50	100	450x75
	8x1	Leaderboard 728x90	8:1	Medium	600x75	1200x150	150	300	1200x150
	10x1	Super Leaderboard/ Pushdown 970x90	10:1	Large	900x90	1800x180	200	400	1800x180
Vertical	1x2	300x600	1:2	Large	300x600	450x900	200	400	450x900
	1x3	Portrait 300x1050	1:3	X Large	300x900	450x1350	250	500	450x1350
	1x4	Skyscraper 160x600	1:4	Medium	160x640	240x960	150	300	240x960
Tiles	1x1	Medium Rectangle 300x250	1:1	Medium	300x300	450x450	150	300	450x450
	2x1	120x60 Financial	2:1	X Small	200x100	300x150	50	100	300x150
	9x16	N/A	9:16	Large	300x540	450x800	200	400	450x800

The above ad formats are displayed in pixels (px), however, the most recent update from the IAB has changed these ad formats slightly.

IAB New Ad Portfolio

In July 2017, the Interactive Advertising Bureau (IAB) released a finalized version of the new standard, known as *IAB Standard Ad Unit Portfolio* which was the biggest update since 2002 and supersedes the universal ad package (UAP).

The Ad Unit Portfolio has been enriched with ad units allowing for each creative to adjust to a variety of screen sizes and resolutions.

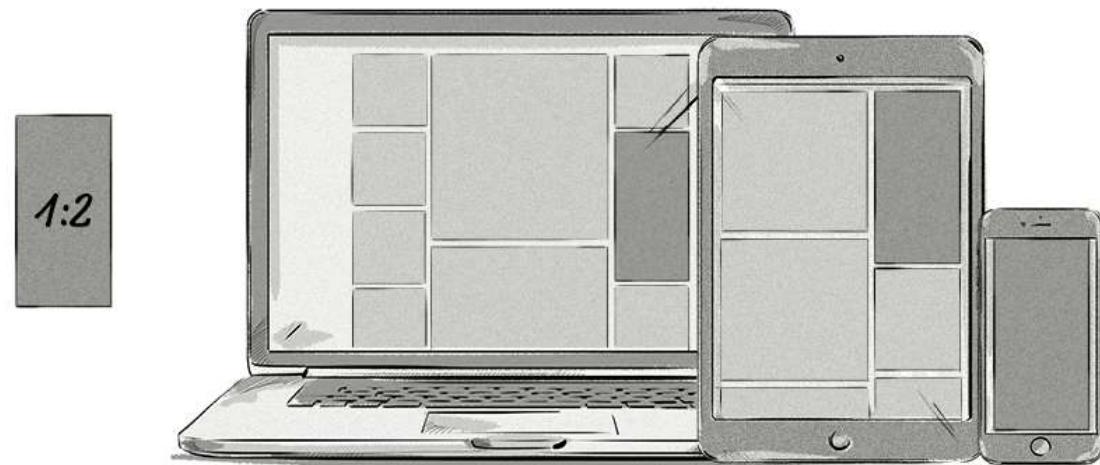
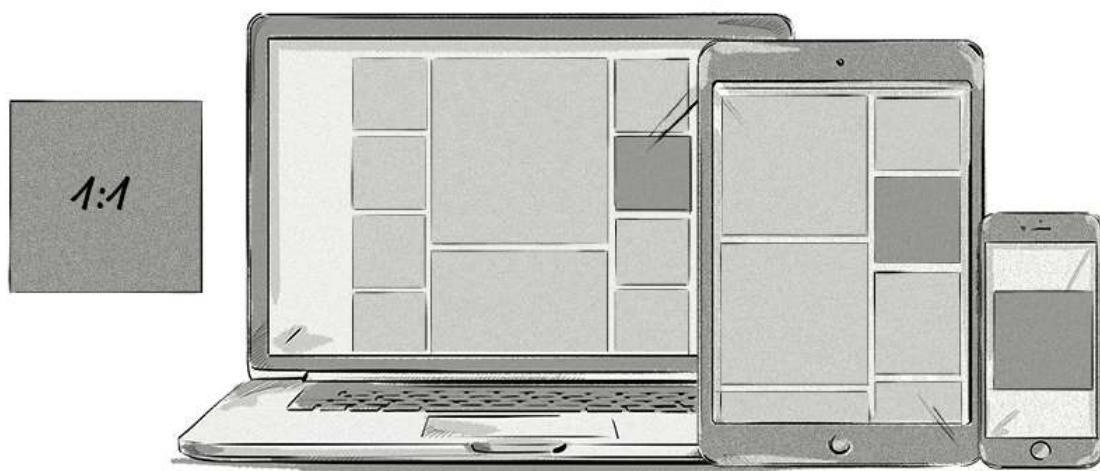
The ad units now include ad sizes based on aspect ratio rather than on specific sizes in pixels, and incorporate the LEAN Principles:

Lightweight

Encrypted

AdChoices supported

Non-invasive ads across mobile, display, and native ad formats.

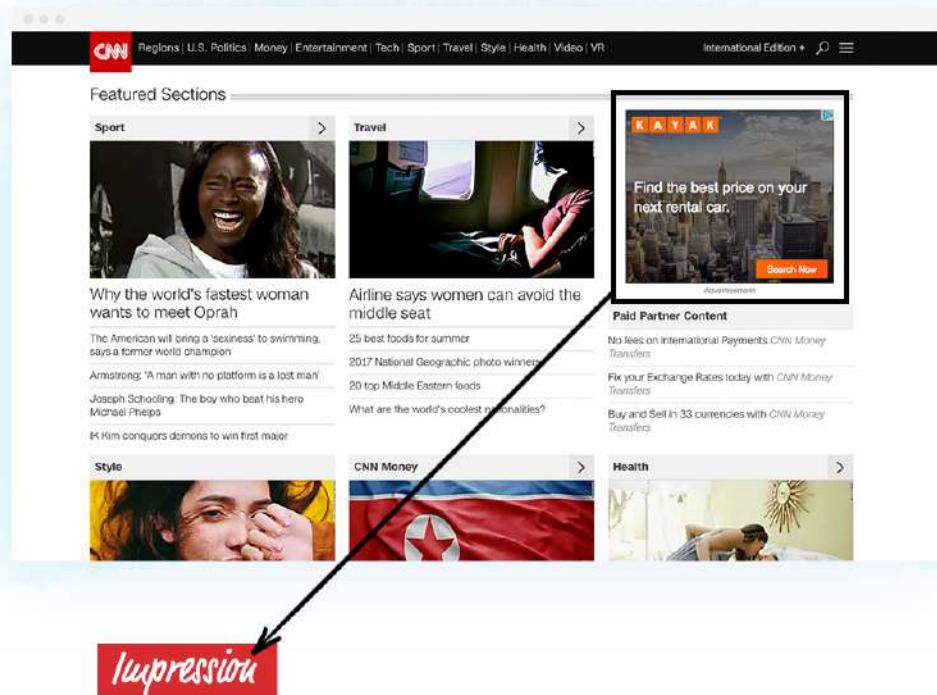


The above images illustrate the difference between ads that have an aspect ratio of 1:1 and 1:2. The current IAB ad formats consist of nine aspect ratios. Learn more at iab.com

The aspect-ratio feature allows ads to adjust to match various screen sizes and resolutions. The IAB's new ad portfolio is based on HTML5 and also includes guidelines for augmented reality (AR), virtual reality (VR), social media, mobile video, emoji ad messaging, and 360-degree video ads.

Impression

An **impression**, also sometimes referred to as an **ad view**, is counted every time a creative is served.



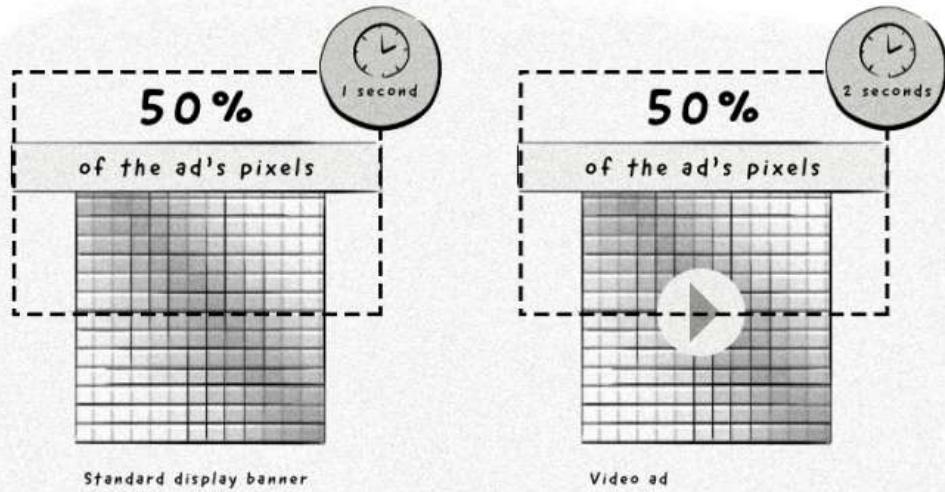
It's important to note that if a user refreshed the page and saw the exact same ad, then another new impression would be counted.

See chapter **06. Ad Serving** chapter to learn more about impressions and how they are tracked.

Viewable Impression

A **viewable impression** is a metric used to determine whether an impression was actually seen by a real human or whether it was “seen” by a bot or hidden from the user’s view—for example, at the bottom of the page where the user doesn’t scroll.

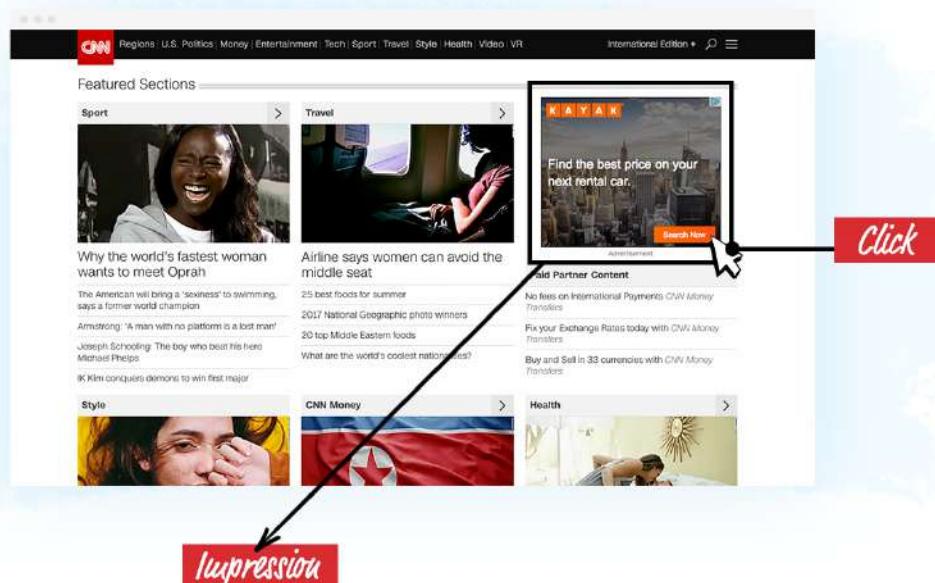
The below chart shows when an impression is deemed viewable according to the standard [set by the IAB](#):



Please refer to chapter 13. **Ad Fraud and Viewability** chapter for more information about viewability.

Click

A **click** is counted when someone clicks on an ad, even if the person doesn't reach the advertiser's website, for example, if it's temporarily unavailable.



Conversion

A **conversion** is counted every time a user completes a goal set by an advertiser or marketer.

For example, a goal could be to get consumers to purchase a product, sign up for an online service, download a file like an ebook, or even fill in a contact form on a landing page.



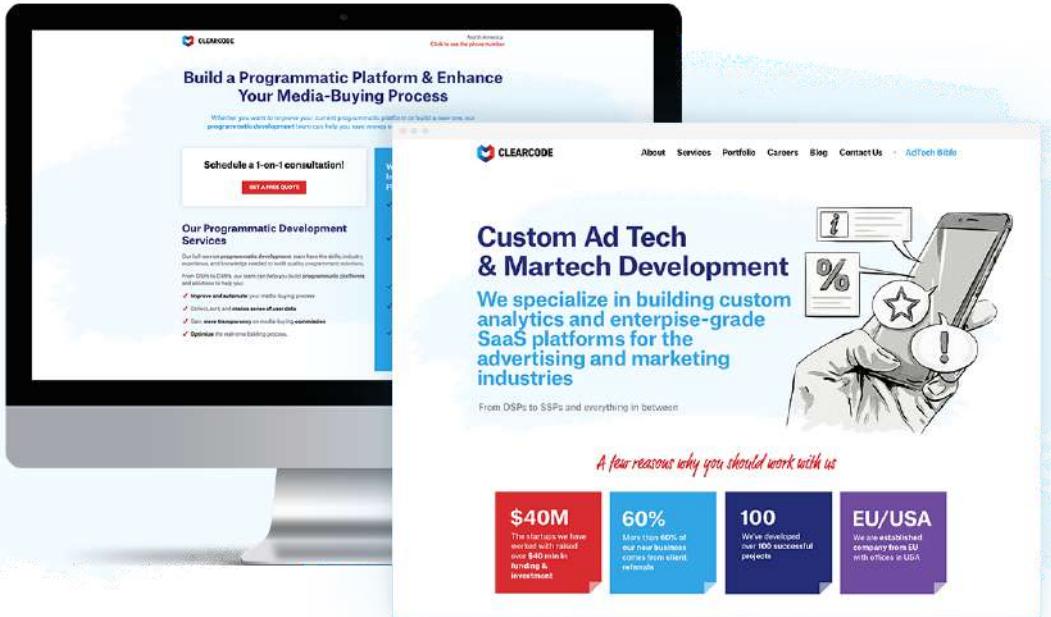
The form on the left represents the goal – get visitors to download the free guide – and the graph on the right represents the number of conversions per month (how many times the free guide was downloaded).

Landing Page

A **landing page** is a web page that an online user “lands on” after clicking on an ad or link.

Landing pages are designed to be different than the usual pages of an advertiser’s website, as they are built with a single objective in mind—get the user to convert and complete a goal, like the ones mentioned above.

Advertising campaigns usually direct traffic to landing pages to increase the number of conversions, especially when it’s a direct-response or prospecting campaign.



The page on the left is a dedicated landing page, as it has one common theme (programmatic media-buying development services) and one common goal (schedule a one-on-one consultation). The page on the right is the homepage and has a more general theme with a number of different navigation options.

Effectiveness of a Campaign

Throughout this book, you will see us talk about the *effectiveness of an advertising campaign*.

This refers to meeting the goals and objectives of the campaign, whether that be increasing the number of conversions and sales or traffic to the advertiser's landing page or website.

Pricing Models

There are a few ways advertisers pay to show their ads on publisher sites.

Cost Per Mille (CPM)

The CPM pricing model refers to the cost per 1,000 impressions; the word *mille* is Latin for one thousand.

The reason we use thousands instead of individual impressions is that the price per impression is very small compared to clicks or conversions and it would be cumbersome from an accounting perspective if the advertiser paid \$0.002 per impression.

Even though the calculation in ad servers and DSPs is done on a per-impression cost (e.g. \$0.002 per impressions), the CPM formula is presented to the advertiser, publisher, or AdOps team so that's easier for them to calculate.

Cost Per Click (CPC)

Cost per click is a pricing model used to express how much each click on an ad or link would cost the advertiser.

If an advertiser buys ad inventory from a publisher on a CPC basis of \$1.10, then every time a visitor clicks on the ad, the advertiser is charged \$1.10.

Cost Per Action/Acquisition (CPA)

With this model, the publisher or affiliate only receives payment from the advertiser when a user has converted (e.g. purchased a product or filled in a lead form) as a result of viewing or clicking on an ad. This model is often applied in affiliate networks and isn't as popular as the CPM or CPC models.

Advertisers generally choose the pricing model based on their advertising strategy. For example, if an advertiser wants to gain brand awareness on a large scale, it would likely choose the CPM model. If it wanted to increase conversions, it would probably go for either the CPM or CPA model.

Did You Know?

You can get estimates on current display advertising figures, including CTR, ad format performance, vertical performance, etc., using [Google's Display Benchmark tool](#).

Chapter Conclusion

This concludes the list of the most important terms.

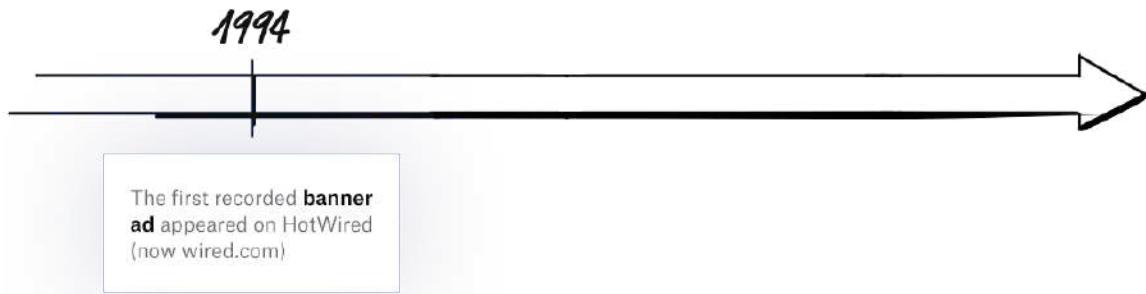
There will be other phrases, acronyms, and vocabulary that will appear in this book, but we'll introduce them using the light-grey information boxes as well as link them to our [AdTech Glossary](#).

03. The History of Online Advertising Technology



Advertising Moves Online

It was during the early 1990s when many companies, organizations, and Internet enthusiasts started creating the first public websites. Advertisers soon spotted the potential that this new world had to offer and began testing uncharted waters.



The year 1994 saw the first recorded example of online display advertising in the form of a banner ad, which appeared on a website called HotWired (now wired.com). It was purchased by telecommunications giant AT&T and used to promote its campaign titled **You Will**.

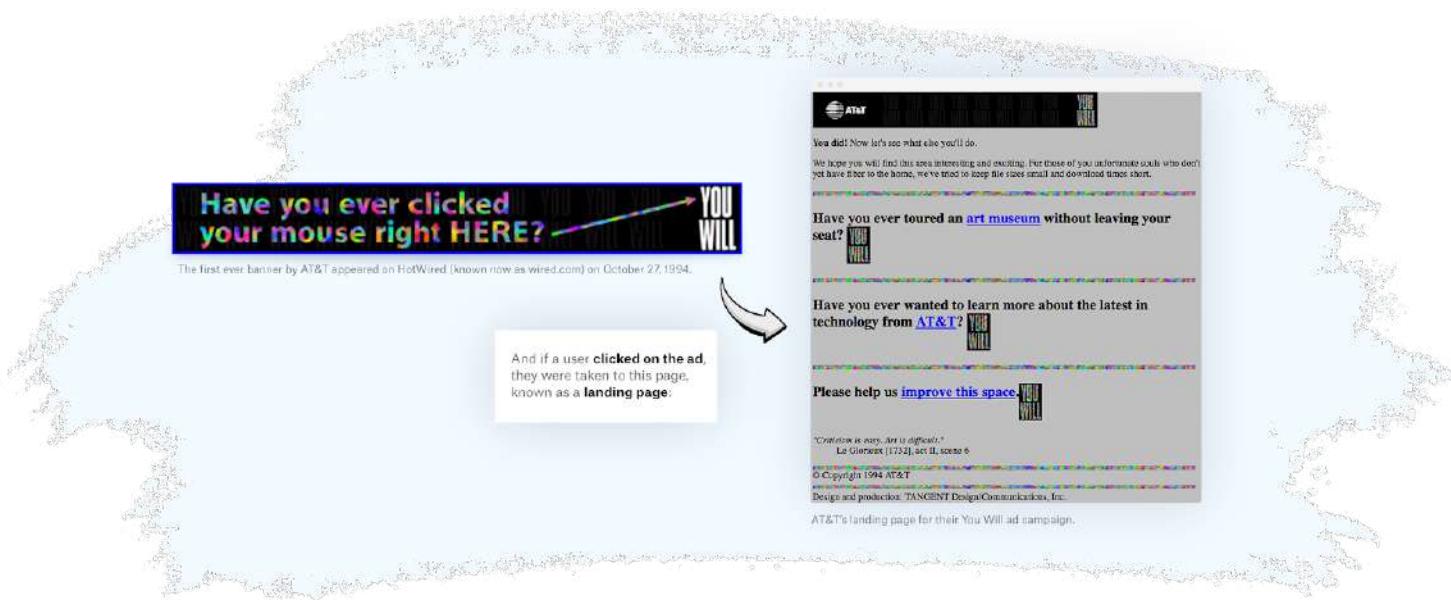


Image on the left: The first ever banner ad by AT&T appeared on HotWired on October 27, 1994.

*The image on the right: AT&T's landing page for its **You Will** ad campaign.*

Over its three-month life span, **44% of viewers clicked on the banner ad**; compare that to today, where it's estimated that online visitors click on about 0.02% to 2% of ads.

What is click-through rate? (CTR)

Click-through rate (CTR) is the number of clicks an ad receives divided by the number of times it's displayed. For example, if an ad had a CTR of 2%, then for every 1,000 impressions, it received 20 clicks.

This was the beginning of what is now a highly lucrative trade.

In the early days of online display advertising, the exchange between an advertiser and a publisher was a direct sales process and resembled the way media had always been bought and sold.

The advertiser would contact the publisher and purchase ad space on its website on a cost-per-thousand basis, known as [Cost Per Mille \(CPM\)](#), as mille means *thousand* in Latin. This system meant advertisers would pay a certain price for every 1,000 impressions (i.e. 1,000 views).

In order to display ads on a publisher's website, the advertiser would send an insertion order (IO) to the publisher's sales team. The insertion order defines the terms of the campaign and includes the following:

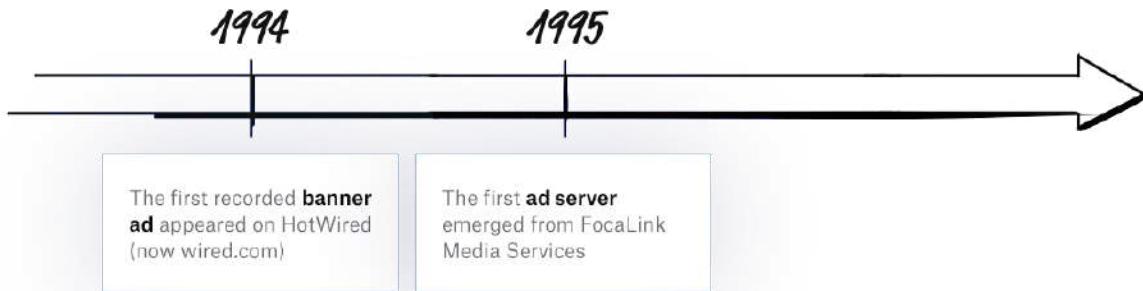
- **Campaign objectives:** Target group, traffic, branding, etc.
- **Line items with campaign execution terms:** Which banner sizes to use, where to place the ads, and which pages to display the ads on.
- **Business terms:** The pricing model (CPM, CPC, etc.) and payment terms.

Did you know?

The terms **insertion order** and **line items** have their roots in print advertising. Orders were made for "insertions" of the ads in newspapers and the advertiser paid a given rate per line. For example, a single insertion of a three-line item of Business Notice in the *The New York Express* in 1870 cost 60 cents.

Source: [Pettengill's Newspaper Directory and Advertisers' Handbook](#)
[S. M. Pettengill & Company, 1870:](#)

This was still a manual process that wasn't utilizing the potential that online advertising had to offer. That all changed when the first-ever piece of advertising technology emerged—the [ad server](#).



The first ad servers began popping up in 1995 and initially were used to control the delivery and management of online ads.

Back then, their targeting capabilities were very limited; they could only target ads based on the header information that was passed along with an HTTP call from the user's browser, such as:

- The language set on the user's computer
- The URL of the page the ad is being loaded onto
- The browser type and version
- The user's operating system

The first-ever ad server

The first-ever ad server was founded by a company known as FocaLink Media Services in 1995 by Dave Zinman, Andrew Conru, and Jason Strober.

The company's name was changed to AdKnowledge in 1998 and was acquired in 1999 by CMGi.

Interestingly enough, CMGi was an Internet company in the 1990s and owned many well-known tech and online businesses, with AltaVista being one of its major portfolio companies.

Even though CGMi survived the dot-com crash in the late 1990s and early 2000s, they sold AltaVista in 2003 to Overture Services, Inc, which was taken over by Yahoo in the same year due to mounting pressure from the board of directors following the 9/11 terror attacks and subsequent stock-market crash.

After some time, difficulties started to arise when the number of websites, and therefore publishers, began to increase. The once-straightforward direct sales process started to become more complex and drawn-out.

While premium ads—those bought by advertisers directly from the publishers—were still common, publishers soon found that a lot of other available inventory wasn't being filled and fell victim to oversupply.

Moreover, advertisers had to sign individual insertion orders with every publisher they wanted to work with and coordinate the campaign execution.

To overcome these problems, [**advertising networks \(aka ad networks\)**](#) started to appear. In 1996, a company called DoubleClick emerged as one of the first ad networks.

A brief history of DoubleClick

DoubleClick was founded in 1996 by Kevin O'Connor and Dwight Merriman. It was purchased by private equity firms Hellman & Friedman and JMI Equity in July 2005 for US\$1.1 billion. Then, in March 2008, it was acquired by Google for US\$3.1 billion.

DoubleClick was one of the few online companies to survive the dot-com bubble between the mid-'90s and early 2000s.

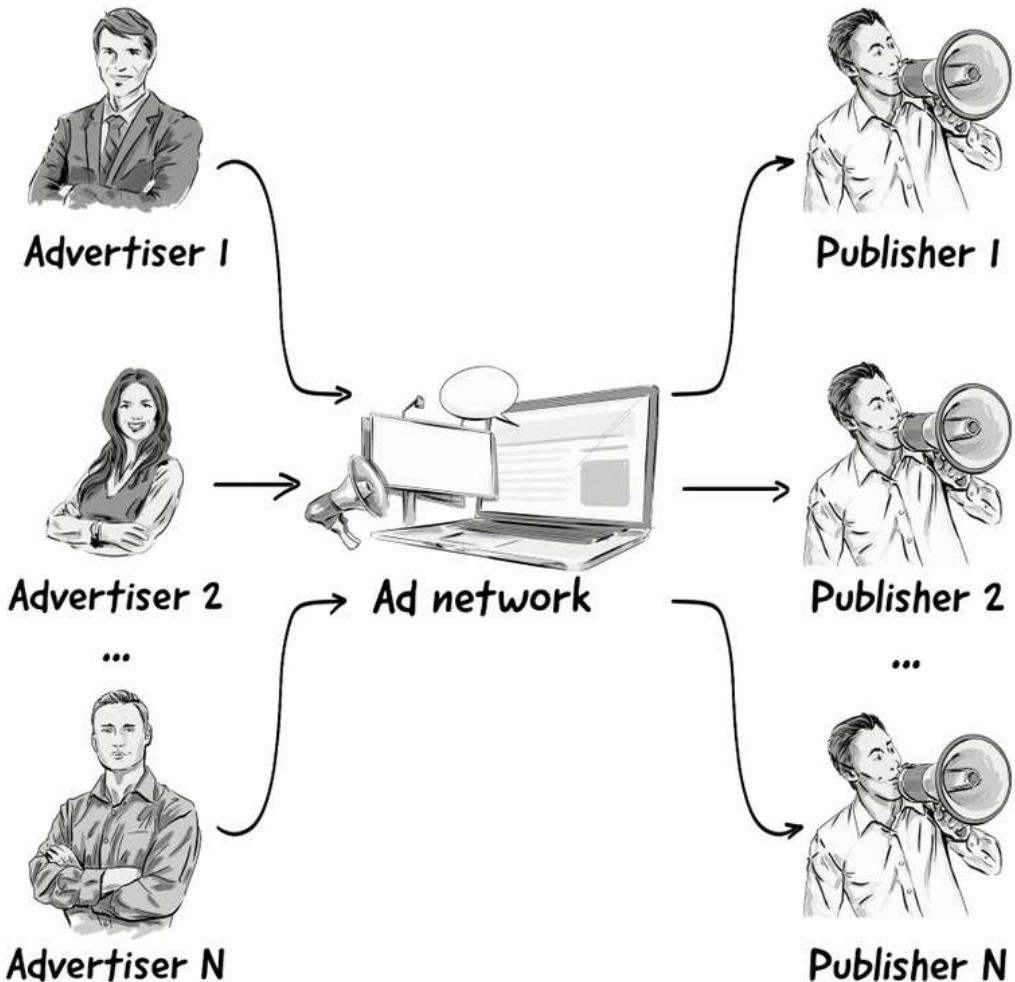
In 2018, [Google rebranded their Google AdWords and DoubleClick ad products](#) and created three primary

brands: Google Ads, Google Marketing Platform, and Google Ad Manager.



In the beginning, ad networks acted as brokers between advertisers and publishers and enabled publishers to monetize their inventory without the need for in-house sales or [AdOps](#) teams.

They would aggregate unsold inventory from publishers and offer advertisers a consolidated and generally less expensive pool of impressions.



Ad networks benefit both advertisers and publishers.

They provide publishers with a highly effective way to sell their remnant inventory, which could be as little as a few percent to all of their inventory, depending on how many direct deals they have with advertisers.

They also help cut down on the time and money associated with selling inventory to advertisers and offer a range of services, such as campaign setup, optimization, and technical support (aka troubleshooting). These services are known today as ***ad trafficking***.

Advertisers benefit by receiving high cost savings and an easier, more effective way to connect with audiences on a much larger scale.

However, even though the introduction of ad networks added fluency to the ad buying and selling process, many ad networks only wanted to purchase part of publishers' inventory (i.e. the parts that matched their campaigns) which meant publishers had to work with multiple ad networks in order to sell all of their inventory.

Not only did this mean publishers would have to spend more time searching for the best-valued ad networks and pay multiple commissions, it also meant they would have set up the inefficient and tedious [waterfall](#) system.

For advertisers, this also created challenges. They soon found that they weren't able to reach their target audience by using just one ad network, so they started buying inventory from multiple ad networks. However, this meant they often bought the same audience more than once, lacked clear insights into the effectiveness of their ads, and struggled to identify their best-performing inventory.

To overcome these challenges, a new AdTech platform arrived on the scene – **network optimizers**, which are known today as [supply-side platforms \(SSPs\)](#).

Network optimizers allowed publishers to:

- Eliminate the time-consuming task of managing multiple ad networks.
- Improve page-load time by sending a single request to a network optimizer rather than sending requests back and forth between the ad networks and the publisher's ad server (i.e. the waterfall technique).
- Increase revenue by matching their inventory to the right ad network.
- Maintain strict quality controls by blocking certain advertisers, e.g. ones that advertised taboo products and services, such as tobacco and alcohol.

Shortly after the introduction of network optimizers, [ad exchanges](#) emerged to solve the many technical nuisances found in ad networks, such as multiple redirects, and allowed advertisers to purchase inventory on an impression-by-impression basis. Ad exchanges were one of the AdTech platforms involved in the invention and growth of [real-time bidding \(RTB\)](#).

This was how the online advertising industry looked in the early days – a handful of AdTech platforms helping advertisers and publishers explore the possibilities that technology and the internet had to offer.

Fast forward to today and the online advertising ecosystem consists of numerous platforms that have arisen over the years to solve the many challenges both advertisers and publishers have faced and to improve the overall buying and selling of digital media.

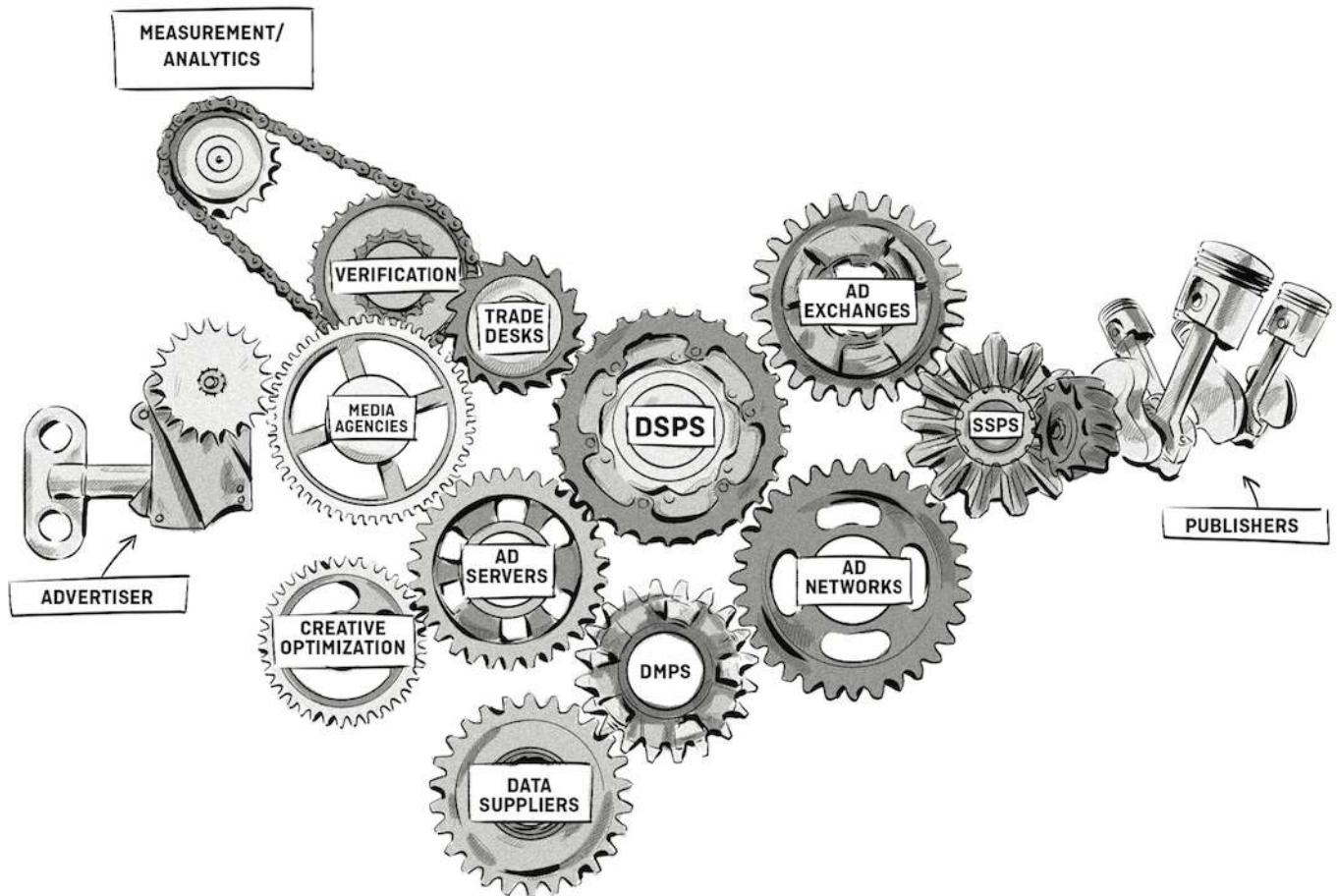
A timeline of the most important events in programmatic advertising

Below are a few important events from the first decade or so.

- **1994:** Lou Montulli and John Giannandrea invent cookies while working at Netscape.
- **1994:** AT&T displays the first ever banner ad on HotWired (now Wired).
- **1995:** The first ever ad server was founded by a company known as Focalink Media Services. The company was founded by Dave Zinman, Andrew Conru and Jason Strober.
- **1996:** Kevin O'Connor, Dwight Merriman and Fergus O'Daily found DoubleClick.
- **1996:** Yahoo! starts displaying search ads on their search engine.
- **2000:** Google launches AdWords (now known as Google Ads). It started with a cost-per mille (CPM) pricing model, but later introduced a cost-per click (CPC) model in 2002.
- **2002:** Applied Semantics creates AdSense contextual advertising technology. Google acquired the company in April 2003 and launched the Google AdSense network, enabling publishers to monetize their content with pay-per click (PPC) ads.

- **2006:** Popular ad-blocking software, Adblock Plus, launches.
- **2007:** Mobile ad networks, like AdMob, emerge and start selling ad space on mobile phones. This was before the smartphone era with the first iPhone being released a year later in 2007.
- **2007:** Google acquires DoubleClick for \$3.1 billion, Microsoft buys AdECN for reportedly between \$50-75 million, and Yahoo! purchases RightMedia for \$700 million.
- **2007/2008:** Real-time bidding (RTB) is introduced as a way to allow advertisers to buy individual impressions on websites via a real-time auction. It's around this time that demand-side platforms (DSPs), like [MediaMath](#), start to emerge.

04. The Main Technology Platforms and Intermediaries in the Online Display Advertising Ecosystem

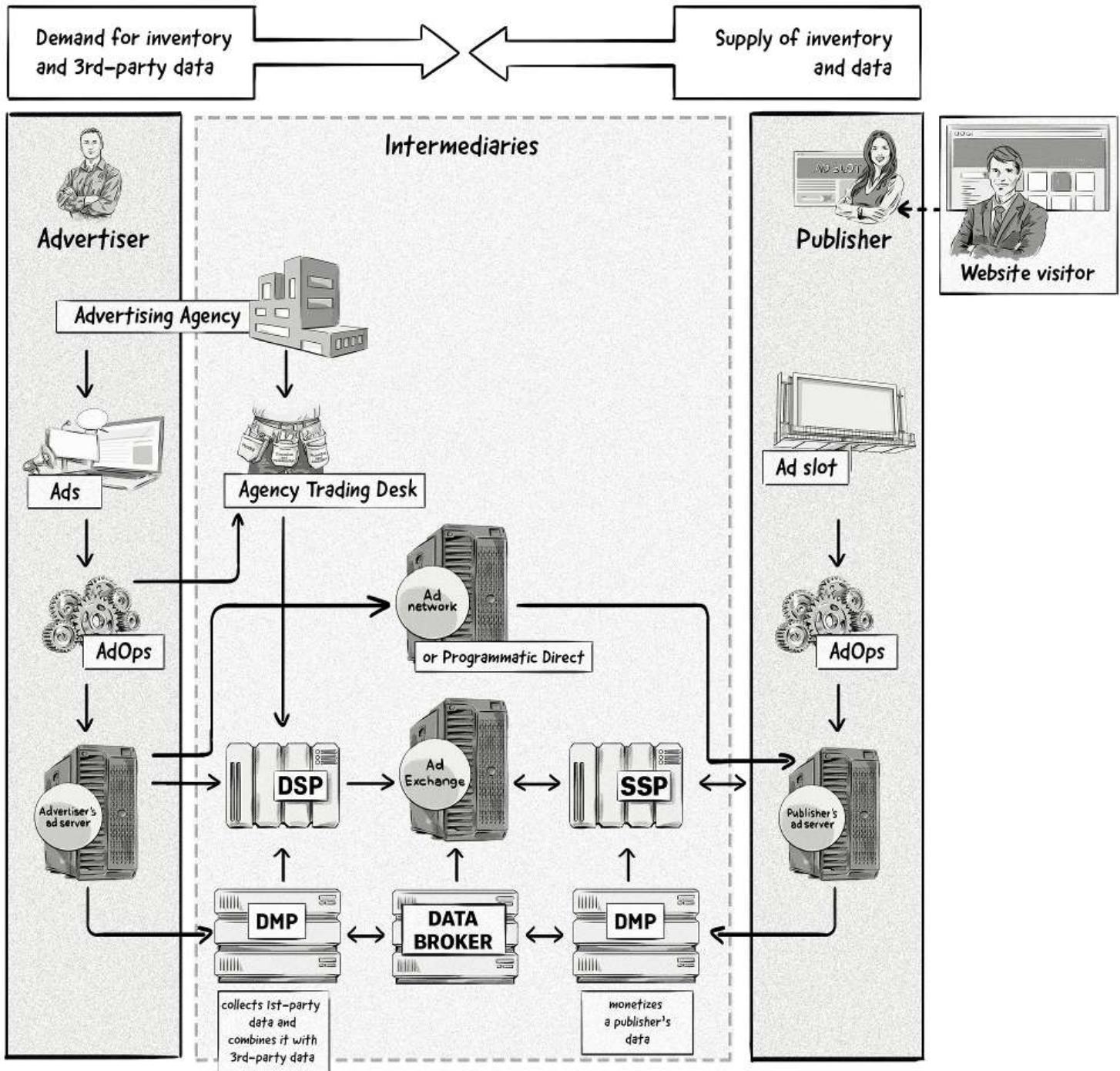


As we learned in the second chapter, advertising in the offline, print world before the introduction of the Internet was a manual process that relied on people to create, configure, and deliver advertising campaigns.

The Internet has brought with it, however, a revolution of technological innovation that has changed the way all of these things are done.

Today, online and some offline advertising campaigns are produced by technological platforms (software). These platforms are all part of the **online advertising ecosystem**.

The online advertising ecosystem is a vast entity that consists of over a dozen **different types of advertising technology platforms** and **intermediaries** that all play a role in the creation, execution, and measurement of an online advertising campaign.



A brief overview of the online advertising ecosystem.

As the diagram above illustrates, there are a number of platforms and intermediaries involved in the buying and selling of ads and data.

We'll be constantly referring to these platforms and intermediaries throughout this book, so let's take a closer look at them now.

Advertisers – The Buy Side

Advertisers (brands) represent the buy side, as they are the ones wanting to buy online media (aka ad space or inventory).

Advertising Operations (AdOps)

On the advertiser's side, the AdOps department is responsible for setting up, monitoring and optimizing campaigns.

In the beginning, this was a manual process, but as time went on, AdOps started using AdTech platforms to improve the processes, such as an ad server (aka third-party ad server).

Advertiser's Ad Server (aka Third-Party Ad Server)

A third-party ad server, also known as the advertiser's ad server, is a web-based technology platform responsible for making decisions about what ads to show on a website, serving those ads, connecting with other AdTech platforms (e.g. demand-side platforms) to purchase inventory, and collecting and reporting data such as impressions, clicks, etc.

Below are some examples of standalone ad servers for advertisers:



Intermediaries

Intermediaries are companies and platforms that sit somewhere in between the advertiser and publisher.

Advertising Agencies

An advertising agency is a company that provides services to brands associated with creating, planning, and managing advertising campaigns.

Advertising agencies are generally independent, external companies working for their clients, which can include businesses, international corporations, non-profit organizations, and governments.

Traditionally, brands hired ad agencies to produce television commercials and run print campaigns in magazines, newspapers, and on billboards, but also to take care of other forms of promotion and marketing.

Due to the growth and rise in popularity of the internet, agencies use an array of advertising and marketing technologies to create, run, manage, and measure online campaigns. These types of agencies are also known as interactive, creative, media, or digital agencies.

The History of Advertising Agencies

Before advertising agencies were born, ads were delivered to various media outlets through representatives who, in the early days of advertising, sold and re-sold advertising space with a markup.

These were the humble beginnings of fully fledged advertising companies, i.e. agencies.

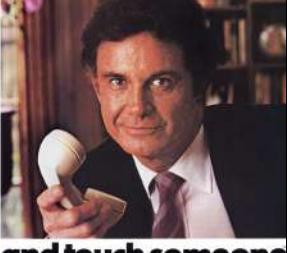
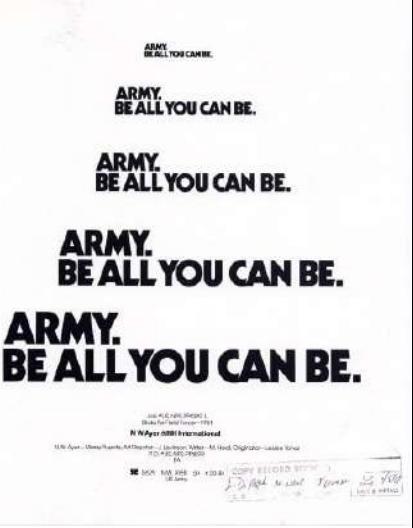
With time, the agencies would take on additional responsibilities: planning, writing, designing, and coordinating ads.

The first bona fide agencies date back as far as 1786 when William Taylor opened his office in London, today acknowledged as the [first advertising agency in history](#). However, while the UK business is considered the precursor of advertising agencies in Europe, it was Volney B. Palmer who took the idea across the ocean to the US.

Palmer opened the first agency on American soil in 1840. [Adland: A Global History of Advertising](#) cites Palmer describing the services he provided using the term “agent”: “the duly authorized agent of most of the best newspapers of all the cities and provincial towns in the United States and Canada, for which he is daily receiving advertisements and subscriptions.”

In this way, Palmer’s office at the northwest corner of Third and Chestnut Street in Philadelphia became the prototype for today’s advertising agency. In 1842, he bought large amounts of space in various newspapers at a discounted rate, then resold the space at higher rates to advertisers. The actual ad, including the copy, layout, and artwork, was prepared by the client, which basically made Palmer an ad-space broker with little influence on the creative side.

Some agents created directories with advertising rates of newspapers and agencies made a profit buying newspaper space and reselling it with a markup. The business model was very popular until the 19th century when [N.W. Ayer & Son](#) was founded in New York. The agency provided a wider range of services, which included planning, creating, and executing complete campaigns, making itself famous working for brands such as [De Beers](#), [AT&T](#), and the U.S. Army, creating [a number of memorable ads and slogans](#):

 <p>The more you hear the better we sound.</p> <p>What would long distance service be if it were not available often at selected hours. If there were no operator service, no person-to-person or collect calling, no immediate service for writing numbers... We know one thing. You wouldn't be AT&T. Calling anywhere. Anytime. Long distance operators. Day after day. A century of commitment. That's AT&T. The more you hear the better we sound.</p> <p>AT&T Reach out and touch someone</p> <p><small>National Broadcast Oct 1960</small></p>	 <p>ARMY. BE ALL YOU CAN BE.</p> <p>ARMY. BE ALL YOU CAN BE.</p> <p><small>Joe McNally, DIAFOTO, Studio 500, New York City - 1981 WPA Project - Photographic</small></p> <p><small>100% Virgin U.S. Polyester Yarn - 100% M-Hard Polyester - Leader Thread T.O. #4C 400-29500 COPY RECORDED BY L.D. Read to Client, T. Givens, G. Voss 100% Virgin U.S. Polyester Yarn - 100% M-Hard Polyester - Leader Thread T.O. #4C 400-29500</small></p> <p>Military service advertisement for the U.S. Army by E. N. J. Carter 1981.</p>	 <p>ARMY. BE ALL YOU CAN BE.</p> <p>ARMY. BE ALL YOU CAN BE.</p> <p><small>A girl's joy, blooming like a rose, is radiant and full in the lovely miracle of love blossoming. And for her a star, blindingly brilliant, a diamond, the most precious gemstone. Her engagement diamond, fair spark of eternity, reflects the light of her happiness to chandelier splendor, and transmits the timeless message of love until the end of time.</small></p> <p>a diamond is forever</p> <p><small>De Beers Group of Companies</small></p> <p>An advertisement for De Beers diamonds. The term '<i>diamonds are forever</i>' was coined by Mary Frances Gerety 1947.</p>
---	---	--

How Have Ad Agencies Changed Over Time?

In the early days, agencies were hardly creative at all.

Even today, the creative process is actually only a small part of what ad agencies do. [Ogilvy argues](#)¹, on top of the creative side of things, agencies do lots of market research, prepare detailed media plans, and purchase advertising space.

Over the decades, agencies have evolved to suit the changing needs of the clients, doing many things people loosely classify as marketing. The advent of the Internet, however, completely redefined their role and posed new challenges.

Before the Internet

The first advertising agents acted, either directly or indirectly, on behalf of newspapers rather than directly for advertisers.

As such, they were initially only intermediaries selling space and charging hefty commissions on ad space.

However, from their beginnings in the 1800s, through the golden era of advertising in the 1950s, globalization, and the ultimate shift towards digital, ad agencies have gained new roles and diversified.

Already in the Mad Men era of the 1960s, the agency acted more as the brand's partner, taking responsibility for developing strategies, conceiving campaign ideas, and managing the ad insertion process for the brand.

The introduction of the internet

¹ Ogilvy, D. (2011). *Ogilvy on advertising*. London: Prion.

For a long time, agencies were the go-to businesses for all offline advertising efforts. However, the introduction of the internet was a complete game-changer.

AdTech companies started disrupting and threatening the way ad agencies operated by offering completely new opportunities, which shifted the balance of power away from traditional agencies.

Soon, agencies were able to leverage advertising technology, gaining access to unparalleled amounts of data about consumers and their online behavior.

While many brands still think of ad agencies in traditional terms, specialized agencies increasingly explore the opportunities offered by social media, display ads, retargeting, and content personalization.

Today, AdTech companies build complex technologies for brands and advertisers, such as demand-side platforms (DSPs). These types of media-buying tools offer targeting and analytics unheard of in the world of traditional advertising.

Examples of Large, International Ad Agencies

Globalization of advertising and rapid growth of agencies started in the 20th century when American agencies began opening their overseas offices before the two World Wars.

[McCann Erickson](#), established in New York City in 1902, opened its first European offices in 1927. South American and Australian offices followed in 1935 and 1959, respectively.

Companies such as [J. Walter Thompson](#) adopted a strategy to expand in order to be able to provide their services right where their clients operated.

English agencies followed suit and also started to explore opportunities associated with globalization in the 1960s and 1970s.

Overseas expansion offered access to new markets.

[Saatchi & Saatchi](#), perhaps one of the most iconic English agencies today, was founded in 1970 and rose to international prominence following relationships with clients such as British Airways and Toyota. This allowed them to build a network of offices worldwide.

Below are the five largest advertising agencies:



OmnicomGroup

IPG dentsu WPP

WPP Group, London, \$19 billion
Omnicom Group, New York City, \$15.3 billion

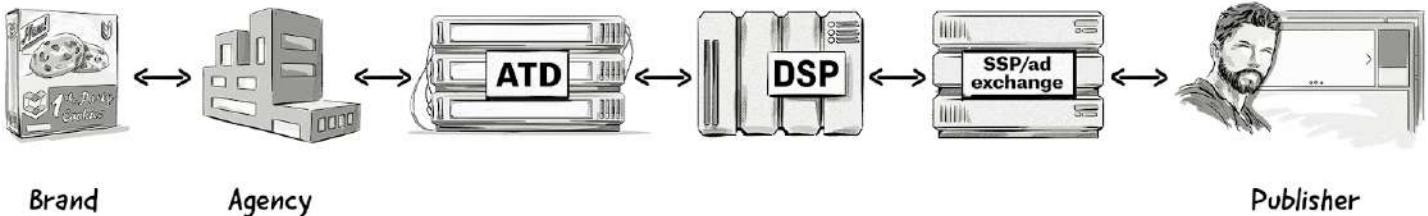
Publicis Groupe, Paris, \$9.6 billion
Interpublic Group, New York City, \$7.5 billion
Dentsu, Tokyo, \$6 billion

Despite the challenges and hurdles ad agencies have faced, especially over the past few years with the rise of AdTech vendors, they have prevailed and proven themselves as a valuable and key component of the advertising process, and will likely remain so for years to come.

Agency Trading Desk (ATD)

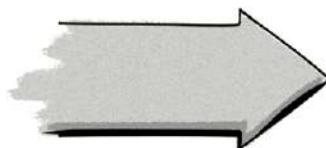
An agency trading desk (ATD) is often defined as a company that offers programmatic managed services to brands.

ATDs are typically responsible for running the programmatic media-buying activities for brands and comprise of both a services layer — media buyers, developers, account managers, etc. — and a technical layer — their proprietary technology plus external tools, such as DSPs.

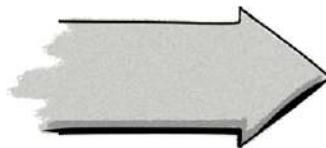
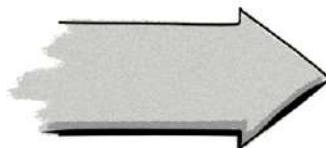
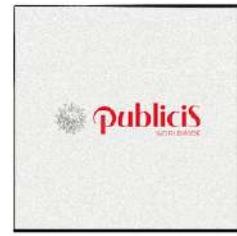
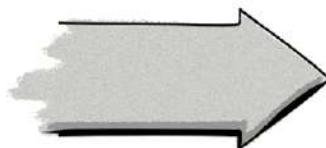
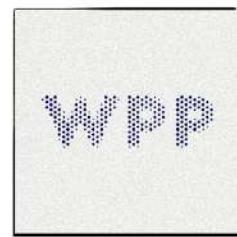
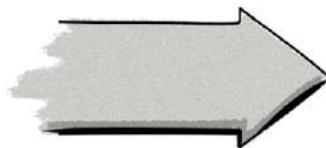


All of the popular advertising agencies have their own agency trading desk which runs the programmatic media-buying activities for the agency's clients.

Agency Trading Desk



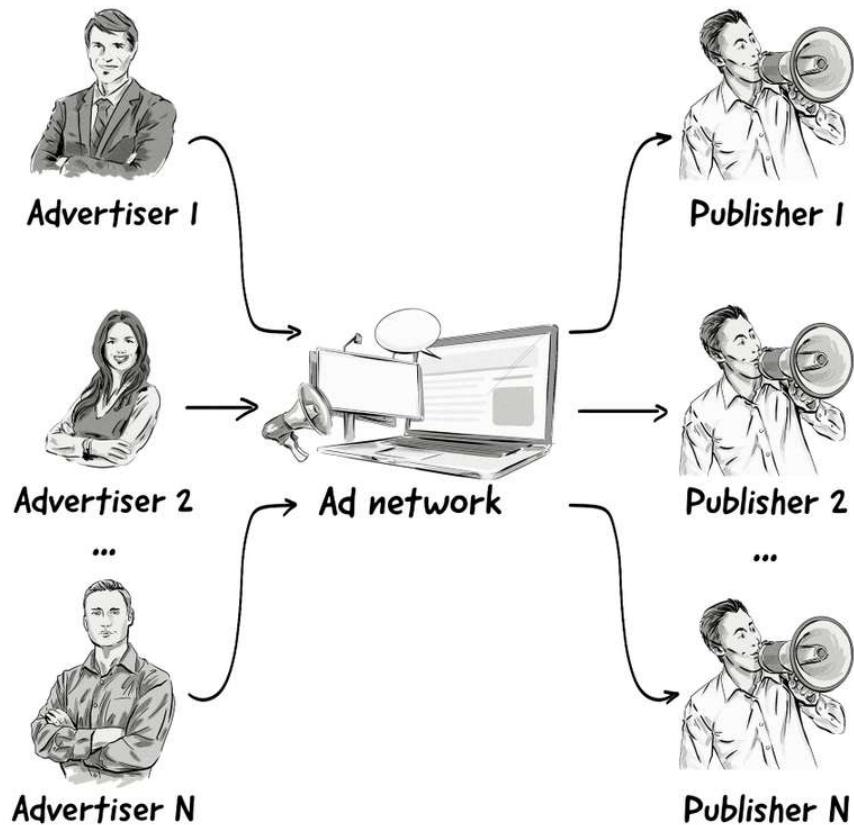
Media Agency



Ad Network

An **ad network** is a technology platform that serves as a broker between a group of publishers and a group of advertisers.

Ad networks were first introduced in the mid-1990s as a way to help publishers sell their available ad inventory and help advertisers scale their digital ad campaigns across many different sites without having to deal with each publisher directly.



Ad networks aggregate unsold inventory from publishers and offer advertisers a consolidated and generally less expensive pool of impressions on a cost-per mille (CPM) basis.

What Benefits Do Ad Networks Provide Publishers and Advertisers?

While ad networks are mainly responsible for helping publishers sell their remnant inventory, they also provide advertisers with some benefits:

Scale: An advertiser can buy more inventory from many publishers through one ad network and centralize the reporting for the campaign.

Time savings: An advertiser sets up the campaign once and does not need to sign insertion orders for each publisher separately.

Campaign reach and measurement: The reach of the campaign will be measured and frequency capping will be applied to the whole campaign.

Monetization: Publishers can sell the inventory that they weren't able to sell via direct deals.

Many ad networks specialize in certain types of inventory, including:

- **Premium ad networks:** Offer inventory from the top publisher brands (e.g. *The New York Times*).
- **Vertical ad networks:** Focus on certain topics, such as business, technology, automotive, fashion, etc.
- **Specialized ad networks:** Focus on a certain type of channel (e.g. mobile, video, native).
- **Performance and affiliate ad networks:** Use the revenue share, cost-per click (CPC), or cost-per-action (CPA) pricing model.

The targeting and decision-making processes in ad networks work in a similar way to those found in ad servers, but there are a few slight differences.

By setting targeting criteria for a campaign, an advertiser can choose which web traffic is relevant for them.

Examples of targeting criteria in ad networks include:

- Run on network (RON) – run on all sites in the ad network
- Run on site (ROS) – target specific domains/publishers in the ad network
- IAB categories
- Geolocation
- Keywords (context)
- Time of day
- Browser type / OS
- ... and many others

Some popular ad networks include:



Undertone

media.net

infolinks

MNItargetedmedia^{inc}

Demand-Side Platform (DSP)

A demand-side platform (DSP) is a technological platform that allows media buyers (advertisers and agencies) to run advertising campaigns and buy inventory from various ad exchanges and SSPs through one user interface.

DSPs are a key component of the real-time bidding (RTB) process, which allows advertisers to buy media on an impression-by-impression basis.

To help improve targeting and enhance media buys, DSPs often utilize data from data-management platforms (DMPs) and data brokers.

Some of the main DSPs on the market are:



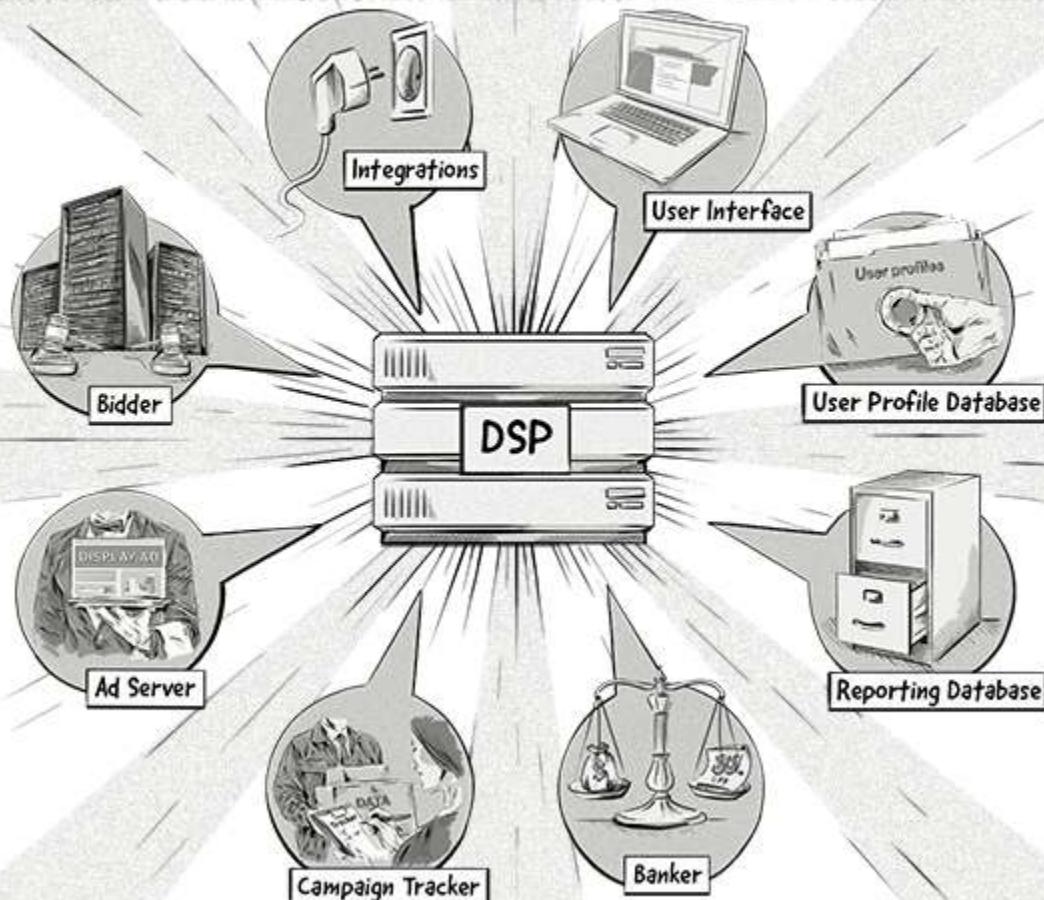
criteo. Sizmek® dataxu®

AMOBEE theTradeDesk®

adform BrightRoll

DSPs are complex platforms that incorporate many different components, including:

The Anatomy of a Demand-Side Platform (DSP)



[Click here](#) to view the full infographic.

What's the difference between an ad network and a DSP?

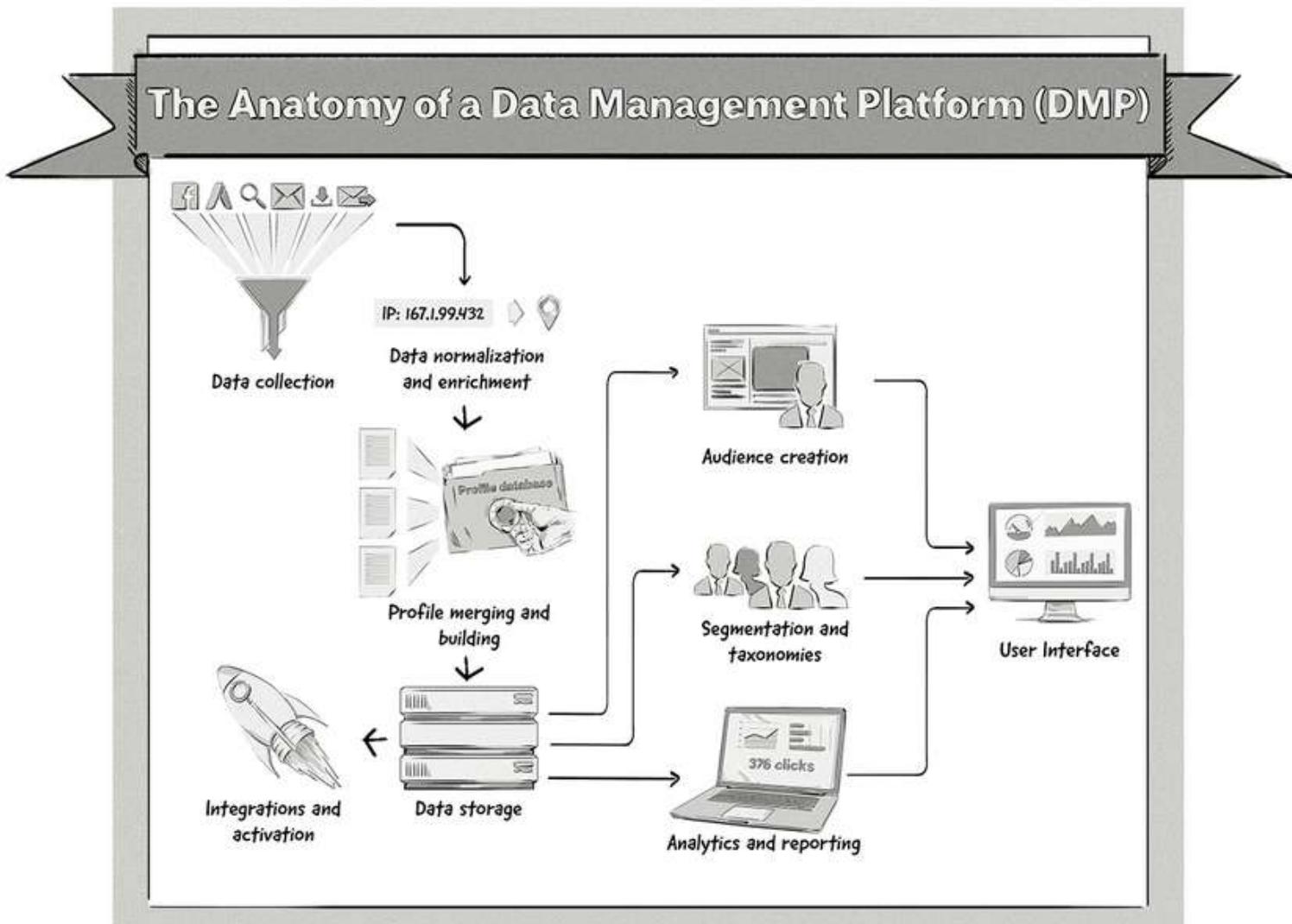
Even though these two platforms seem to operate in a similar way, the main difference is:

Ad networks aggregate inventory from multiple publishers and sell it as packages to advertisers, whereas DSPs purchase inventory on an impression-by-impression basis via real-time bidding (RTB).

Data-Management Platform (DMP) – For Advertisers

A data-management platform (DMP) is responsible for collecting, storing, and organizing massive loads of data for advertisers, taken from a wide range of first-party, second-party, and third-party sources.

The image below illustrates the main features and components of a data-management platform (DMP).



[Click here](#) to view the full infographic.

Advertisers can use a DMP to improve the targeting of their online advertising campaigns. To do this, they would carry out the following processes:

- Collect the data – e.g. first- and third-party data.
- Create audiences based on certain criteria, such as gender, location, or interests.
- Export these audiences to media-buying platforms, such as demand-side platforms (DSPs), and use them for ad targeting.

Below are some popular DMPs:



We explain more about what a DMP is and how it works in chapter [11. Data Management Platforms \(DMPs\) and Data Usage](#).

Ad Exchange

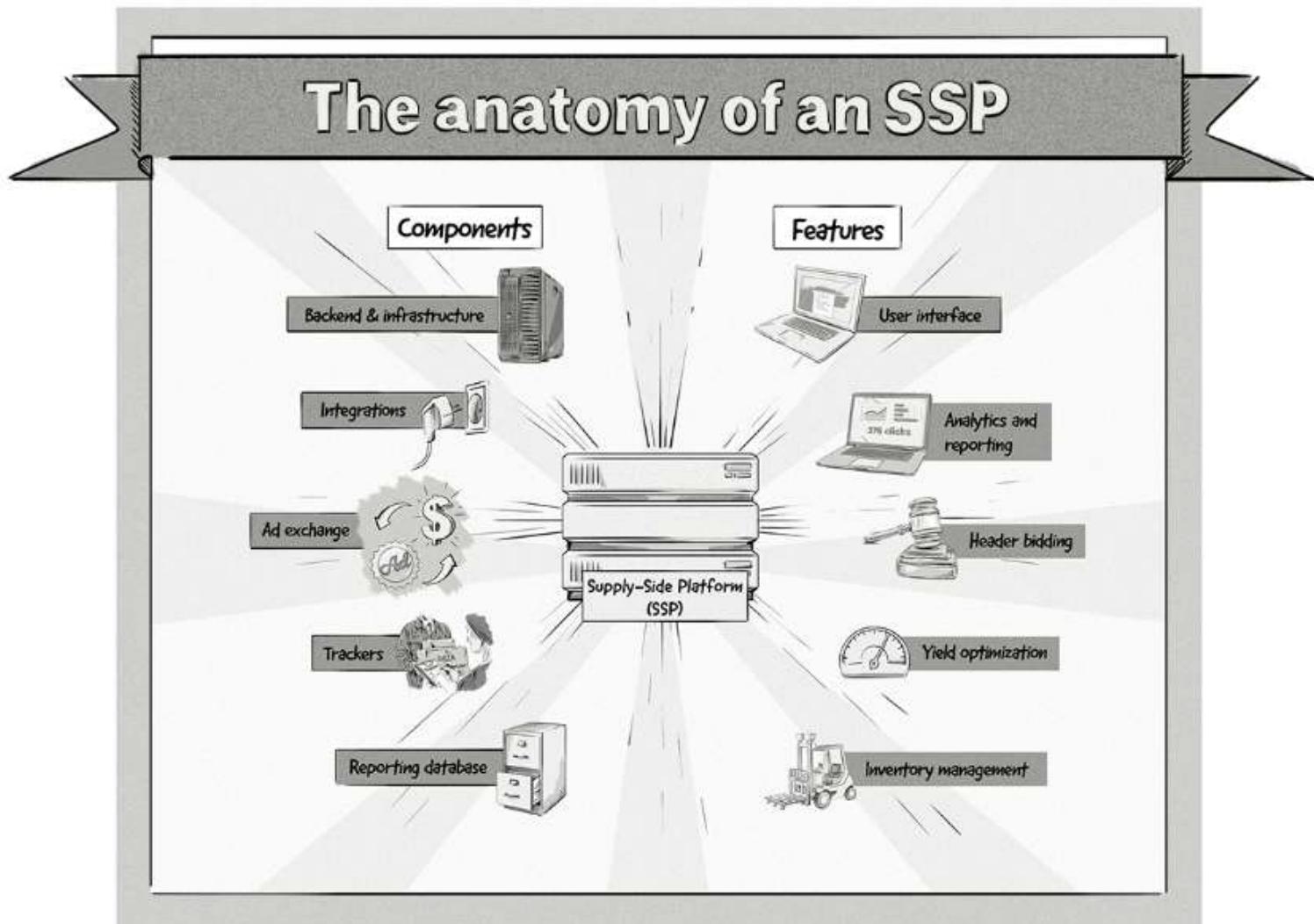
An ad exchange is a dynamic technological platform that facilitates the buying and selling process of available impressions between advertisers, who place their bids via DSPs, and publishers, who sell their inventory via supply-side platforms (SSPs) or directly with the ad exchange.

Ad exchanges are often compared to stock exchanges, as the buying and selling process of media is akin to the process of buying and selling stocks via a stock exchange.

Supply-Side Platform (SSP)

A supply-side platform (SSP) is another technological platform designed to help publishers sell their inventory on multiple ad exchanges and ad networks, and in some cases directly to DSPs, in an automated, secure and efficient way.

The main components and features of an SSP include:



[Click here](#) to view the full infographic.

Even though publishers don't need to use an SSP to sell their inventory on the ad exchange, the technology used in SSPs provides many benefits that allow them to receive the most yield from their inventory and gain clearer insights into their audience.

Some popular ad exchanges and SSPs include:



What's the difference between an SSP and an ad exchange?

In short, SSPs offer their clients tools to help them manage their inventory, sell their inventory on ad exchanges, and optimize yield.

Ad exchanges allow DSPs and SSPs to come together and conduct media transactions, sort of like an eBay for ads.

However, most SSPs nowadays also exchange mechanisms, meaning DSPs can connect directly to SSPs and purchase inventory through RTB auctions. This DSP-SSP connection is achieved by using the OpenRTB protocol (more on that in a later chapter).

Data-Management Platform (DMP) – For Publishers

While data-management platforms have typically been associated with advertisers, they also provide publishers with a number of opportunities.

The main things publishers can do with a DMP include:

- Creating another revenue stream with audience extension.
- Increasing the cost of their inventory.
- Improving engagement with content personalization.

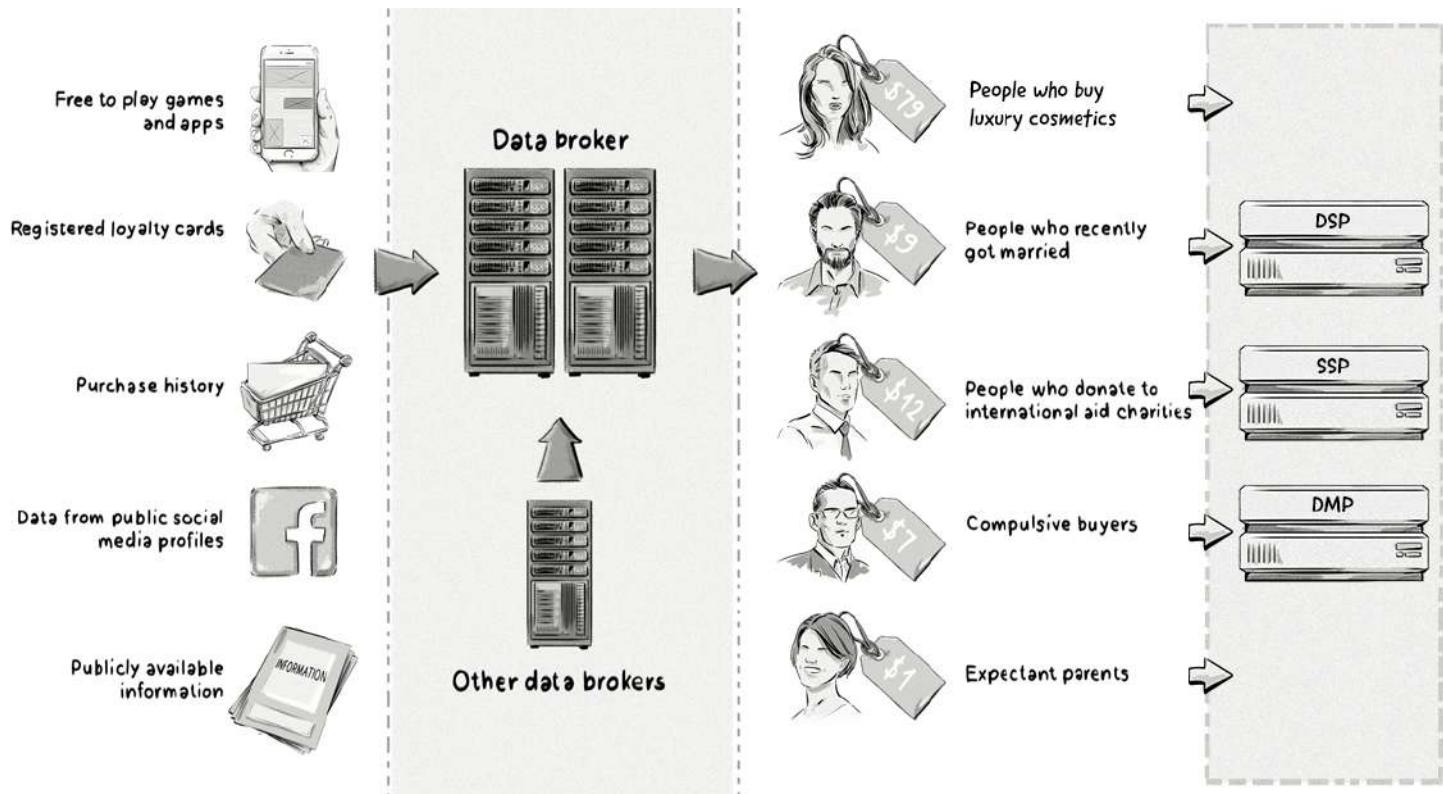
We explain more about what a DMP is and how it works in chapter [11. Data Management Platforms \(DMPs\) and Data Usage](#).

Data Broker

A data broker – also known as an *information broker*, *data provider*, and *data supplier* – collects and sells offline and online consumer data to other companies.

Data brokers buy data from different publishers and other data holders (credit-card companies, telecoms and ISPs, retailers etc.) combine it into aggregated audiences (aka segments).

Segments are most commonly organized into different categories, such as demographics (gender, age, income groups, etc.), interests (sports, travel, etc.), purchase intent (e.g. car/home buyers), and many others.



These segments are then sold to advertisers and used for ad targeting, typically by connecting to demand-side platforms and data-management platforms.

Below are a few of the main data brokers that supply data to advertisers:



comscore



ORACLE®



Verification and Measurement

Verification services use technology to provide advertisers with additional information about their online advertising campaigns.

The information provided by verification services can inform the advertiser about the following:

- On which websites the ads were displayed.
- Where they were displayed (geolocation).
- What percentage of ads were viewable by the user.
- If fraudulent traffic was detected, e.g. impressions, clicks, and/or conversions generated by bots.
- If the ads were displayed next to questionable content (e.g. illegal or offensive content).

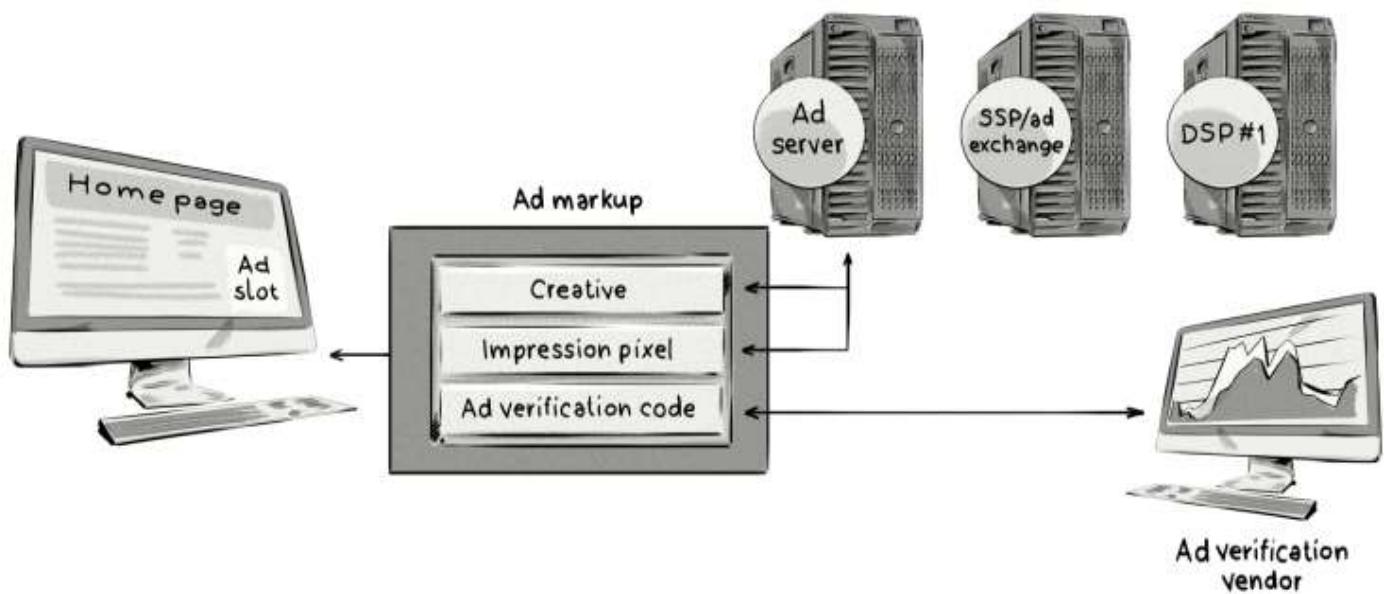
Measurement and analytics companies provide detailed analysis of the performance and reach of online ads. They also provide detailed insights into customer behavior, trends and other user-centric data to help advertisers improve the performance and targeting capabilities of their campaigns.

It's important to note that the analytics mentioned here are different than the analytics used for tracking and reporting on website traffic or in-app user behavior.

Web/app analytics are part of the marketing-technology (MarTech) ecosystem; however, more and more web- and marketing-analytics solutions are providing insights into ad campaigns. This is part of a trend aimed at

providing more robust platforms that combine several functions and cover many different areas connecting both the online marketing and advertising technology spaces.

Here's an overview of how ad-verification tools work:



Here is what's happening in the image above:

- A user opens a web page, which contains a dedicated space where an ad loads (an ad slot).
- Demand-side platforms (DSPs) are called via supply-side platforms (SSPs), ad exchanges and ad networks. When there is a direct publisher-advertiser deal, the ad code (aka ad markup) is configured directly in the publisher's ad server, including the creative, impression-tracking pixel and ad-verification code.
- The DSP with the highest bid wins the impression. An ad is sent to the publisher's site via the ad markup.
- As the ad is loaded, the ad-verification code in the ad markup collects information about the website and user – ad placement, audience, engagement, etc.
- The ad-verification vendor sends performance reports to the advertiser.

Creative Optimization

A creative optimization company works with media buyers (advertisers and agencies) to improve the performance of online ad campaigns.

These creative optimization companies usually add a layer of rich media, such as video, to the standard banner ads to make them more interactive, dynamic, and appealing — thus improving their effectiveness.

Dynamic creative optimization (DCO) platforms utilize user data to personalize the creative and run A/B tests to determine the best-performing variant of the creative — all with minimal human involvement.

The Sell Side (Publisher)

Publishers (websites and apps) represent the sell side, as they are the ones wanting to sell the ad space to media buyers.

Advertising Operations (AdOps)

The AdOps department on the publisher's side is responsible for setting up the advertiser's ad campaigns in their ad server (known as a first-party ad server or publisher's ad server), trafficking tags, configuring header-bidding wrappers and making changes to campaigns if required.

First-Party Ad Server

This technological platform allows publishers to manage the ad slots on their website and display ads that have been sold directly to advertisers (i.e. direct campaigns). In the event that no direct campaigns are available, first-party ad servers will act as a management platform whereby they decide which ad codes (i.e ones from a third-party ad server, SSP, or ad network) to serve in their ad slots.

Does everyone need an ad server?

Short answer: No.

A large majority of publishers would use an ad server, but not every advertiser would.

As most DSPs offer ad-serving capabilities, advertisers could just use a DSP to store and manage their creatives.

It is also possible for publishers to just use an SSP instead of an ad server, as many SSPs also offer ad-serving functionality and allow publishers to run different types of campaigns.

However, publishers benefit from having an ad server, as it allows them to easily change SSP vendors if needed.

Moreover, smaller publishers could just add the ad codes directly into their website, which would eliminate the need to add and manage a new system.

Here are a few popular ad servers for publishers:



How AdTech Companies Make Money

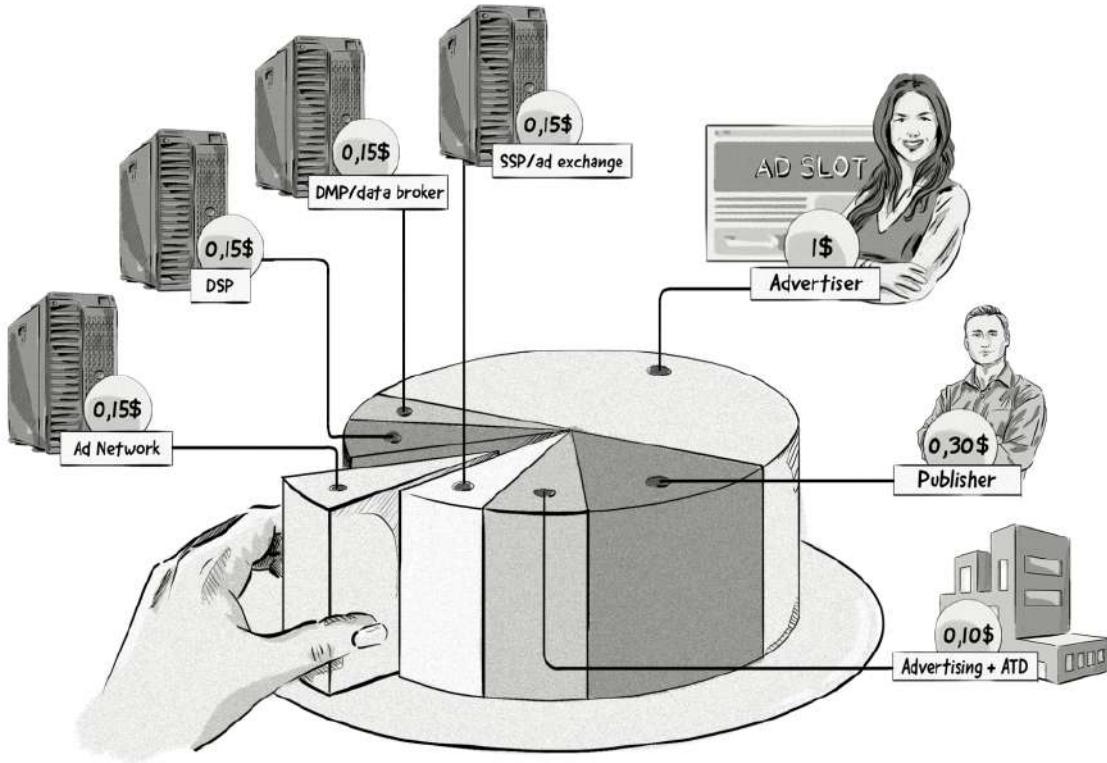
Building and maintaining advertising-technology platforms is a highly expensive exercise with high costs associated with infrastructure and staffing (developers, technical persons, managers, sales teams, etc).

AdTech vendors need to deliver a high-performance product to their clients and ensure their business model makes money along the way to cover costs and make a profit.

Ever since the early days of online advertising, technology providers have made their money by charging commissions and fees, typically as a percentage on top of the cost of media.

Historically, most AdTech platforms added about 30% to the cost of the media, but this number has decreased over the years due to competition and calls for more transparency into the cost of media, as well as fees and commissions (sometimes referred to as the *AdTech tax*).

Many AdTech companies claim their take rates are now in the single digits.



While the above illustration is just an example and every setup is different, this is certainly how an advertiser's budget is distributed a majority of the time.

The AdTech-tax problem is exacerbated due to the fragmented nature of the online advertising ecosystem where there are numerous AdTech vendors involved in the supply chain.

This not only means that advertisers aren't getting their full money's worth, but also that publishers are only receiving a small part of the advertiser's budget.

Over the past few years, the AdTech industry has started to consolidate.

Large AdTech vendors have been acquiring smaller companies and adding them to their client offering.

This plays a role in reducing the number of individual AdTech vendors involved in the online media-buying process, which subsequently reduces the amount of AdTech tax applied to a transaction.

The Walled Gardens

The AdTech ecosystem can be divided into two groups: independent AdTech companies and walled gardens.

The walled gardens refer to the duopoly of Google and Facebook, but increasingly includes Amazon and Apple. You'll likely see them written or mentioned as GAFA = **G**oogle, **A**pple, **F**acebook and **A**mazon.

The reason these companies are called *walled gardens* is because they have closed-off ecosystems, whereby they keep their audience and data to themselves, and require brands to use their advertising platforms to access them.

Here's a quick overview of the power these companies have in online advertising:



Apart from its popular search engine, Google owns many different consumer-facing products that are used by billions of people, including: Google Mail, Google Maps and YouTube.

Google also has multiple advertising products used by advertisers and publishers:



Google Ad Manager (GAM): Includes what was once known as DoubleClick for Publishers (DFP) and DoubleClick Ad Exchange (AdX). This suite allows publishers to manage, sell, and serve their inventory to advertisers.

Google Ads: Previously known as Google AdWords. This is used by brands to buy ads on the Google search engine.

Google Marketing Platform (GMP): Comprising an array of products, including Search Ads 360 (formerly DoubleClick Search), Analytics 360, Data Studio, Optimize 360, Surveys 360 and Tag Manager 360. GMP also includes Display & Video 360 (DV360), which consolidated DoubleClick Bid Manager (DBM), DoubleClick

Campaign Manager, DoubleClick Studio and Google Audience Center 360. GMP is used by advertisers and agencies to purchase ad space from publishers.

Because Google has so many people using its consumer-facing products, which are often accessed via a Google account, it's able to collect data about users and their behavior and offer it to advertisers.



With over 2.3 billion active users, Facebook is a highly attractive option for advertisers wanting to reach their target audience.

Facebook's main ad products include **Facebook's Ad Manager** and **Facebook Audience Network**:

Facebook's Ad Manager programmatically sells only Facebook inventory – based on advertising formats that only appear on Facebook.

Facebook Audience Network allows advertisers to show their ads on mobile apps and websites outside of Facebook, enabling them to reach the same audience on a larger scale.



Similar to Google, Apple also has many popular consumer-facing products, such as the iPhone and Mac computer, which are powered by Apple's iOS operating system.

Apple has also begun launching new services, such as Apple Music, Apple Pay, Apple Video, etc. By offering these products and services to consumers that lack interoperability, the company is growing its market share and a user base that's uniquely its own.

Although Apple runs ads in its App Store, it doesn't have any advertising platforms akin to Google or Facebook, and has taken a rather strong position on user privacy with its [Intelligent Tracking Prevention](#)

feature on its Safari browser and changes to how app developers and AdTech companies can access a user's IDFA on iOS devices.



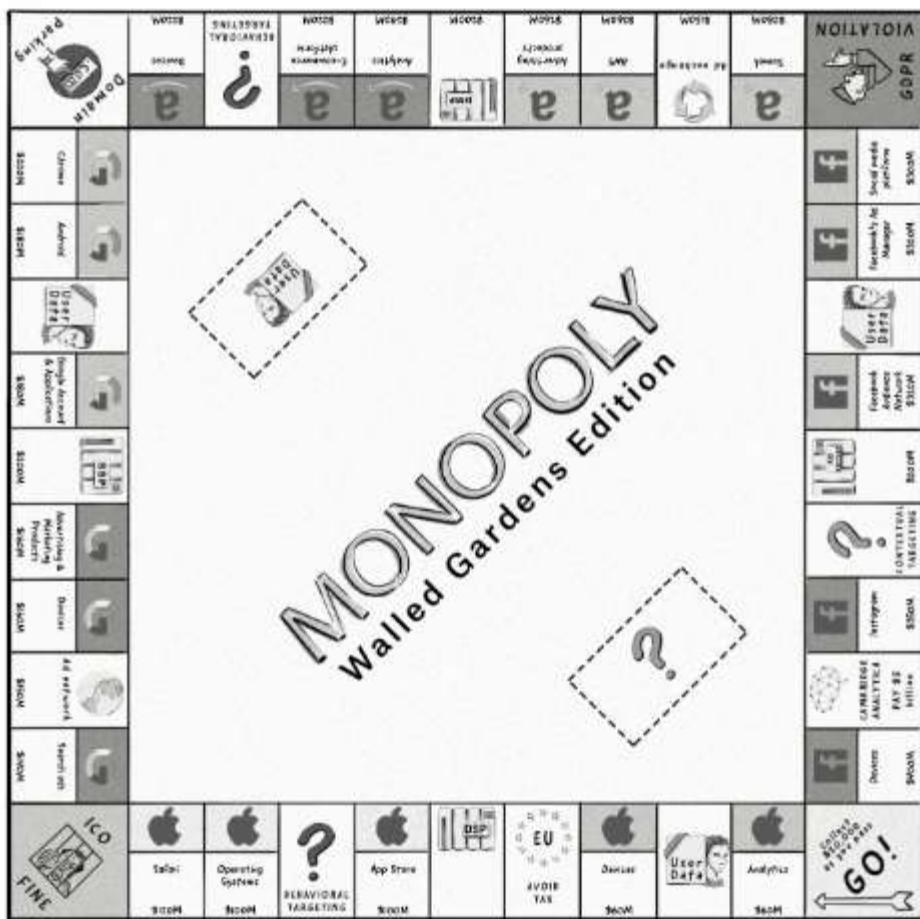
With its large ecommerce business [growing at a healthy pace](#), Amazon has moved into the AdTech business by offering advertisers a way to run ad campaigns via its DSP across its properties; Amazon (ecommerce), Fire, Kindle, IMDb and Prime Video.

Unlike Google and Facebook, Amazon has a treasure trove of data on what people search for and buy, making it an attractive opportunity for retailers.

In 2019, the ecommerce giant expanded its advertising product line by acquiring Sizmek's ad server and dynamic creative tool.

Although this book focuses on the platforms and processes of independent AdTech, we'll refer to GAFA from time to time.

Below is an infographic that we created showing the walled gardens of AdTech and the products they offer:



[Monopoly: The Walled Gardens Edition.](#)

By Clearcode.

Standardization in the Ecosystem

In the very early days of online advertising, it became apparent that there would be a need to provide a set of standards to ensure that different advertising technologies could communicate efficiently with one another and deliver ads in the correct format.

In 1996, the Interactive Advertising Bureau (IAB) was founded as a way to standardize the online advertising industry.



The IAB is responsible for a number of key activities, including developing technical standards, introducing best practices, conducting industry research and educating companies about the importance of online advertising.

As of 2017, the IAB has over 600 members consisting of leading media and technology companies and has 42 international licensee organizations in the IAB Global Network.

Over the years, the IAB has introduced a number of standards to allow seamless communication between those on the buy side and those on the sell side, such as ad formats and protocols.

Throughout this book, we cover and explain a number of standards the IAB has introduced.

05. The Main Digital Advertising Mediums and Channels



Before the Internet existed, brands and agencies used mediums like newspaper ads, direct-mail brochures and TV commercials to push their message to the masses.

Nowadays, they are spoiled for choice with numerous mediums and channels available to them.

What's the difference between a medium and a channel in advertising?

The terms *medium* and *channel* are often used interchangeably.

For example, the Internet could be described as both a medium and a channel.

For the sake of consistency, in this book we'll run with the following definitions:

Medium: A means of verbal or non-verbal communication. Examples include text ads, video ads and radio ads.

Channel: A means of transmission or distribution. Examples include display, social media and TV advertising.

For example, you could create a video ad (medium) and decide to advertise it on Facebook (channel).

Below are the main mediums and channels advertisers have at their disposal in today's digital world.

Advertising Mediums

Text and Image Ads

When advertising moved online in the late 1990s, the only medium available to advertisers was text and image ads.

As we mentioned earlier in the book, this was the first very online ad:



The first ever banner by AT&T appeared on HotWired (known now as wired.com) on October 27, 1994.

Text and image ads now come in many different formats:

Text ads

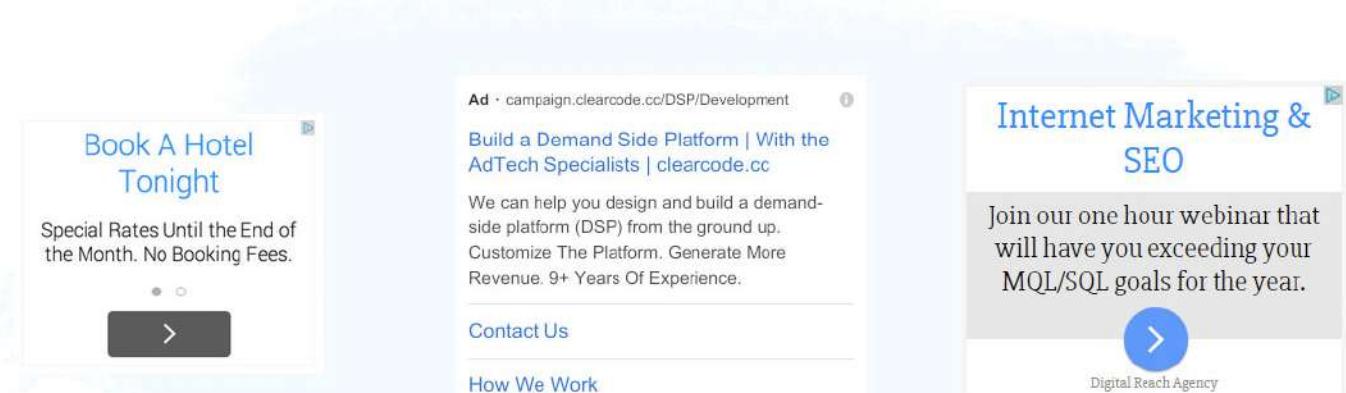


Image ads



Although there have been a number of new mediums released over the years, text and image ads are still the most popular medium for display advertising.

Text and image ads can be served and displayed via HTML, JavaScript, iframe and SafeFrame tags.

Native Ads

Native ads are designed to blend in with the rest of the surrounding content by following the natural form of the user experience and matching the design and behavior of the web page, application, or platform.

Although native ads are meant to look like the surrounding content, they still need to be a clear and prominent disclaimer stating that they are paid advertisements.

Native ads are generally found on content-rich sites, such as news sites, blogs, and social networks.

Here are some of the main native-ad formats provided by the [IAB's Native Advertising Playbook 2019](#):

Content recommendation ads (formerly known as content recommendation widgets): This form of native advertising is probably the most subtle. You may have glanced over this type before and presumed that it is actually content from the website you're reading. However, the telltale sign is the message above the ads, usually written as *From the web*, or *Recommended for you*.



As this type of native advertising appears on content-rich sites, typically at the end of an article.

In-feed or in-content ads: These native ads are similar to content recommendation ads, in-feed and in-content ads. They usually appear in article and content feeds (in-feed ads) and inside articles (in-content ads).

In-Feed Native Ads

In-Feed Native Ads are placed in article and content feeds and mimic the surrounding site design and aesthetics. As consumers scroll the listing of article summaries, editorial is mixed with native ad units providing an uninterrupted flow.



In-Content Native Ads

In-Content Native Ads are ads placed primarily on article pages, in between paragraphs of content or below the article, and are designed in such a way that they mimic the design and aesthetics of the surrounding editorial content experience.

Source: [IAB Native Advertising Playbook 2.0](#)

In-feed and in-content ads come in many forms, such as content (text), image, and video.

Branded/ Native Content: (aka sponsored, brand, or custom content): Unlike the previous two forms of native ads that direct the user away from the site when they click on the ad, branded (aka native) content involves companies paying to show their branded content on a website, like a news site or blog, and is displayed just like the other forms of editorial content on the site.

Some great examples of branded content come from Netflix's ad campaigns promoting the shows *Orange is the New Black* and *House of Cards*:

Women Inmates: Why the Male Model Doesn't Work

As the number of women inmates soars,
so does the need for policies and programs that meet their needs

By Melanie Deziel



Image source: [The New York Times](#)



"IN SOME WAYS NANCY AND I
ARE LIKE ONE HUMAN BEING"

- RONALD REAGAN



Source: [The Atlantic](#)

Creating these types of branded content typically involves collaboration between the brand and the publisher's editorial teams, leading to more creative and engaging content, compared to the other forms of native ads.

Other Forms of Native Advertising

The first version of the IAB's Native Advertising Playbook included paid search and promoted listing as examples of native ads, however, these are no longer classified as native ad types, instead fall under the Search Advertising category listed below.

Video Ads

Video advertising refers to ads displayed in the form of a video, instead of their traditional static form, such as banner ads.

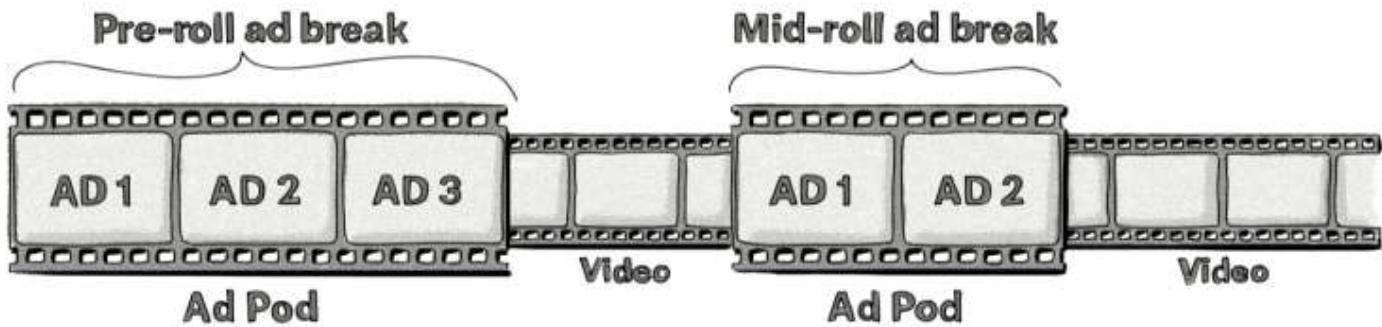
When you think about video advertising, try not to confuse it with television advertising – they are not the same thing, although it's getting more difficult to differentiate between the two because of online streaming services.

Depending on the channel, serving a video ad is similar to serving an image, text or native ad, except that the creative (i.e. the video) is sent to and displayed in a video player rather than as part of the web page itself.

Also, most video ads are served via protocols developed by the IAB Tech Lab, such as **VAST**, **VPAID**, and **VMAP**.

Video ad serving template (VAST)

This protocol solved many of the compatibility issues that advertisers and publishers faced when serving video ads. VAST supports many different types of video formats (e.g. MP4, 3GP, and MOV), can serve pre-roll, mid-roll, and end-roll ads, and provides some interactive functionalities like pausing and skipping ads.



Video player ad interface definition (VPAID)

VPAID allows advertisers to serve rich, interactive ads to users and collect data about how they interact with their video ads, such as if users click different tabs to view more information.

Advertisers can also collect data on whether users engage with different elements, such as filling in a form, completing a survey or even playing a game.

In 2017, the IAB Tech Lab announced that it would retire the VPAID standard and replace it with the Secure Interactive Media Interface Definition (SIMID) for providing interactive functionalities and the Open Measurement Interface Definition (OMID) for attribution.

Here's a look at how these standards can be used for video advertising:

VISION FOR A SIMPLIFIED FUTURE OF DIGITAL VIDEO STANDARDS

DELIVERY

VAST 4 Tags

INTERACTIVITY

"VPAID-interactive"
"VAST Interactive Templates"

VERIFICATION

Open Measurement

 Common to both mobile in-app and browsers

Source: IAB Tech Lab

Video multiple ad playlist (VMAP)

VMAP allows content creators – i.e. those creating the video – to specify where the ad breaks should be placed. This is especially useful for video-content creators who want to control the video experience but don't control the actual video player.

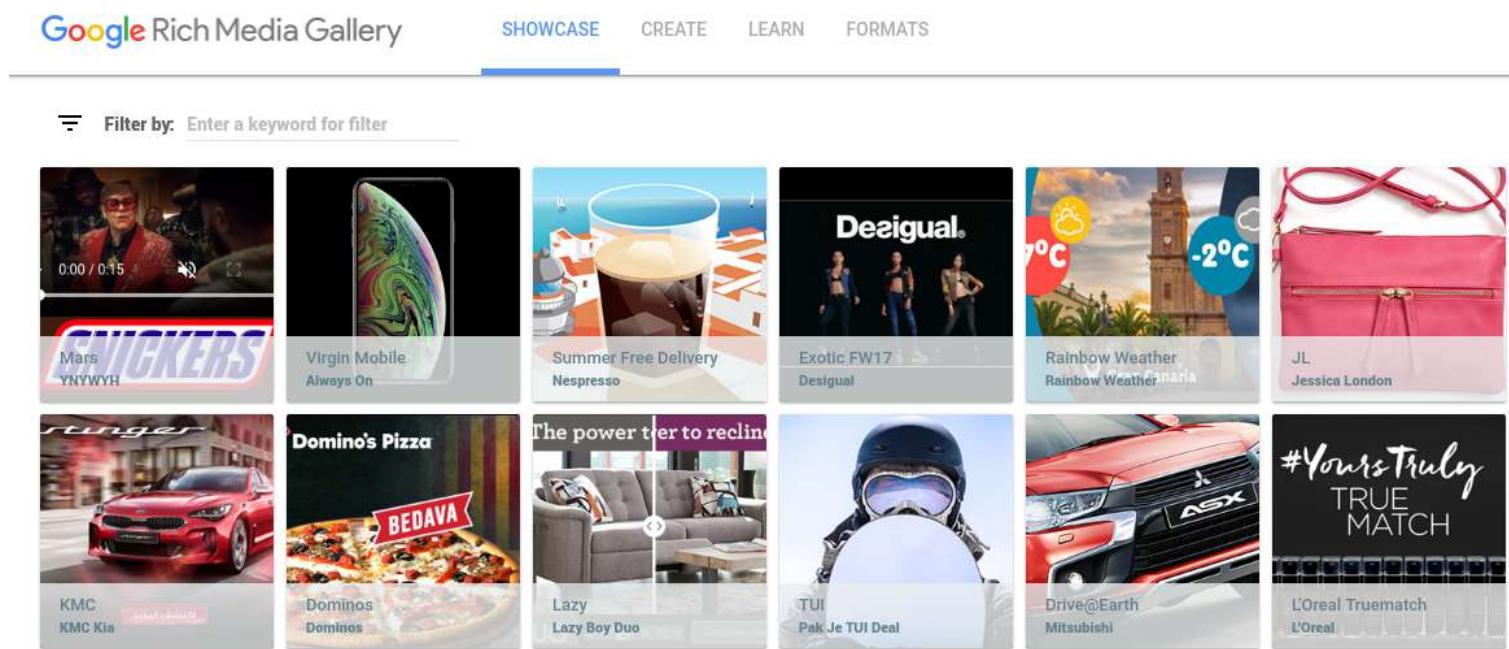
Thanks to VMAP, video-content creators can define the following:

- Ad breaks within their content
- Timing for each break
- How many breaks are available
- How many ads are allowed in each break

Rich Media Ads

Rich media is an interactive form of advertising and can include animated images (e.g. gifs), audio files, and videos.

Unlike traditional text and image ads, rich-media ads often include elements that allow the user to interact with the ad, like the ones listed in [Google's Rich Media Showcase](#):



Rich-media ads come in many [different formats](#), such as:

- **Banners:** Similar to the standard text banners, but with interactive elements.
- **Expanding:** Ads that start off as normal banner ads, but then expand when the user clicks on them. These ads can expand in different directions, such as from right to left or top to bottom.
- **Interstitials:** Rich-media ads that float on top of the page's content.
- **Lightboxes:** These ads are similar to expanding ads in that they expand and often take over the whole screen when a user interacts (e.g. hovers over the ad for at least two seconds) or clicks on the ad.

The ads are typically created and displayed using HTML5 or JavaScript and can utilize VAST or the *mobile rich media ad interface definition* (MRAID) – another IAB standard.

MRAID is an application programming interface (API) used to display rich-media ads in mobile apps.

Because mobile apps can be built using different programming languages and run on different operating systems, MRAID provides a standard framework that allows content creators and advertisers to run rich-media ads across all mobile devices and apps.

Audio Ads

While text, image and video ads have dominated the online-advertising scene for over a decade, new advertising mediums are gaining popularity, with audio ads as a prime example.

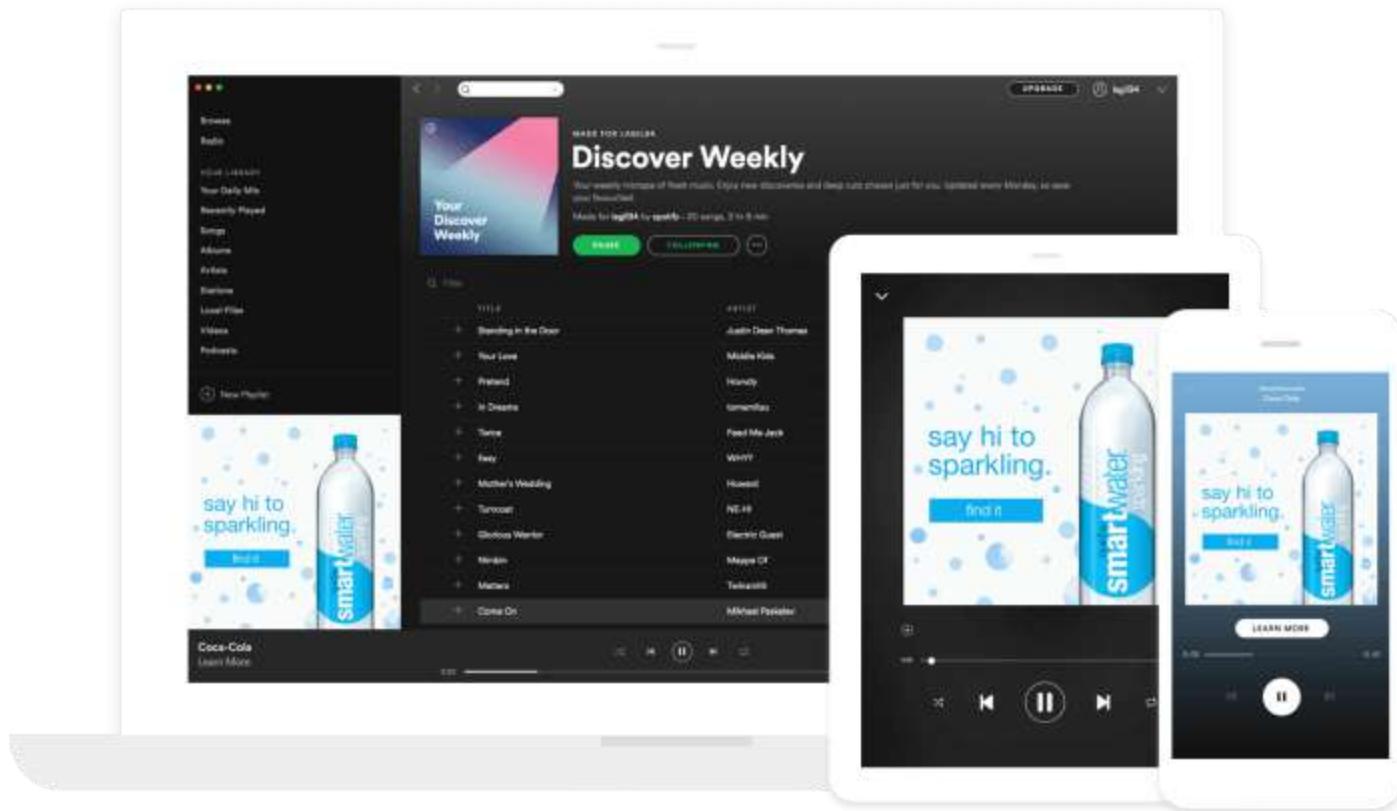
Due to the rise in popularity of podcasts, music-streaming services, and digital radio, audio ads are quickly becoming a new advertising medium for brands and advertisers.

Due to the similarities between video and audio files, publishers and advertisers can use the latest version of VAST (4.1) to serve ads and collect relevant data.

Once upon a time, there was a separate standard for serving audio ads – digital audio ad serving template (DAAST) – but this has since merged into VAST 4.1.

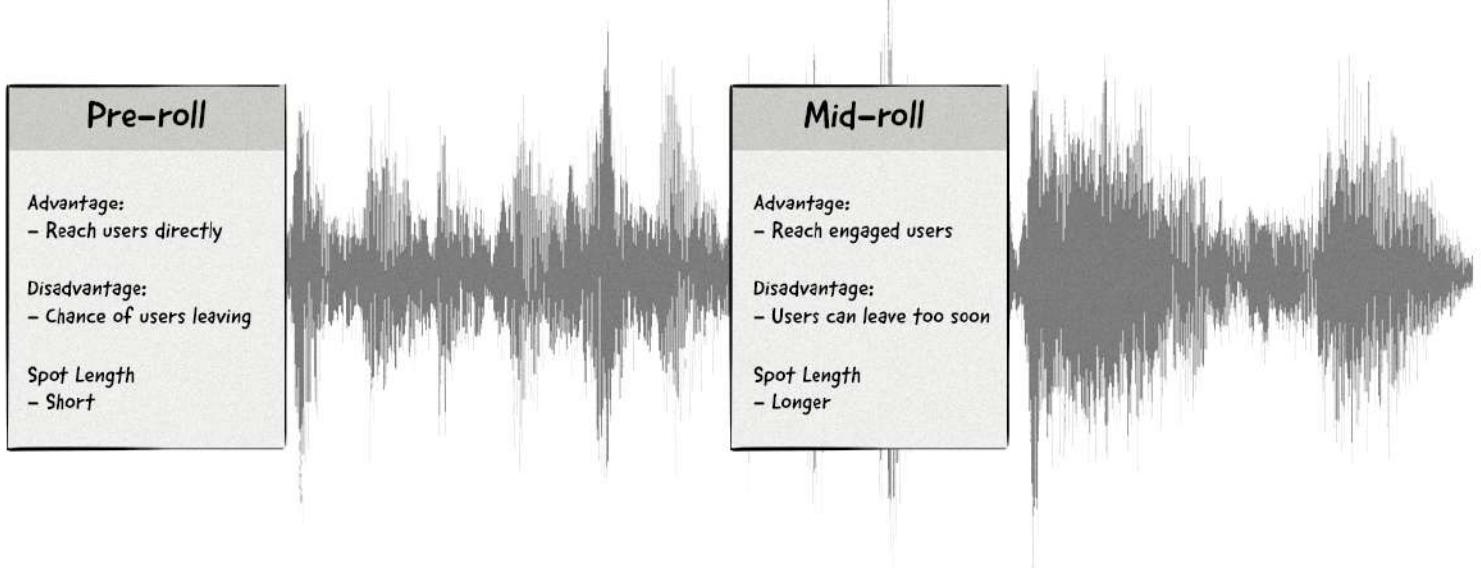
Just like with other digital advertising mediums, audio ads also come in different formats:

Companion/banner ads: Just like the banner ads you see on web pages and mobile apps, companion or banner ads can appear on the screen when the user is listening to an audio track (e.g. a podcast or music).



Source: Spotify

Ad pods: Similar to the ad pods used in video advertising, these can be used to run one or more audio ads in an audio file and can appear as pre-roll (before the content) and mid-roll (in-content) ads.



Source: Clearcode

Dynamic ads: Compared to static audio ads that are designed to announce the same message to the masses, dynamic ads change based on the information known about the user, their location, the time of day, and even the weather.

Advertising Channels

Web Advertising

Web advertising has established roots in online advertising. It was the first channel available to brands and agencies when the world went online back in the late 1990s.

This channel refers to advertisements displayed in web browsers on desktops, laptops and mobile devices (smartphones and tablets).

Displaying ads – whether they are text, image, or video ads – in web browsers involves adding a piece of HTML or JavaScript to a page's content. From there, the web browser will load the ads, along with the rest of the page's content, and display the ads to the user.

The screenshot shows the Cambridge Dictionary website interface. At the top, there are links for Dictionary, Translate, and Grammar. On the right, there are buttons for Log in, English (UK), Follow us (with links to Facebook and Twitter), and a search bar. Below the header, there's a navigation bar with English-Polish, English, Grammar, and English-Spanish options. A sidebar on the left displays an advertisement for a Google Home Max speaker, showing a price drop from \$399 to \$349. On the right, there's a 'My Dictionary' section encouraging users to create and share their own word lists and quizzes.

Translation of "advertising" - English-Polish dictionary

advertising

noun [U] • UK /'ædvətəɪzɪŋ/ US /'æd-ve-təzɪŋ/

B2 the business of trying to persuade people to buy products or services

reklama

an advertising agency



My Dictionary

Create and share your own word lists and quizzes for free!

[Sign up now](#)

[Log in](#)

An example of an image ad promoting the Google Home Max speaker.

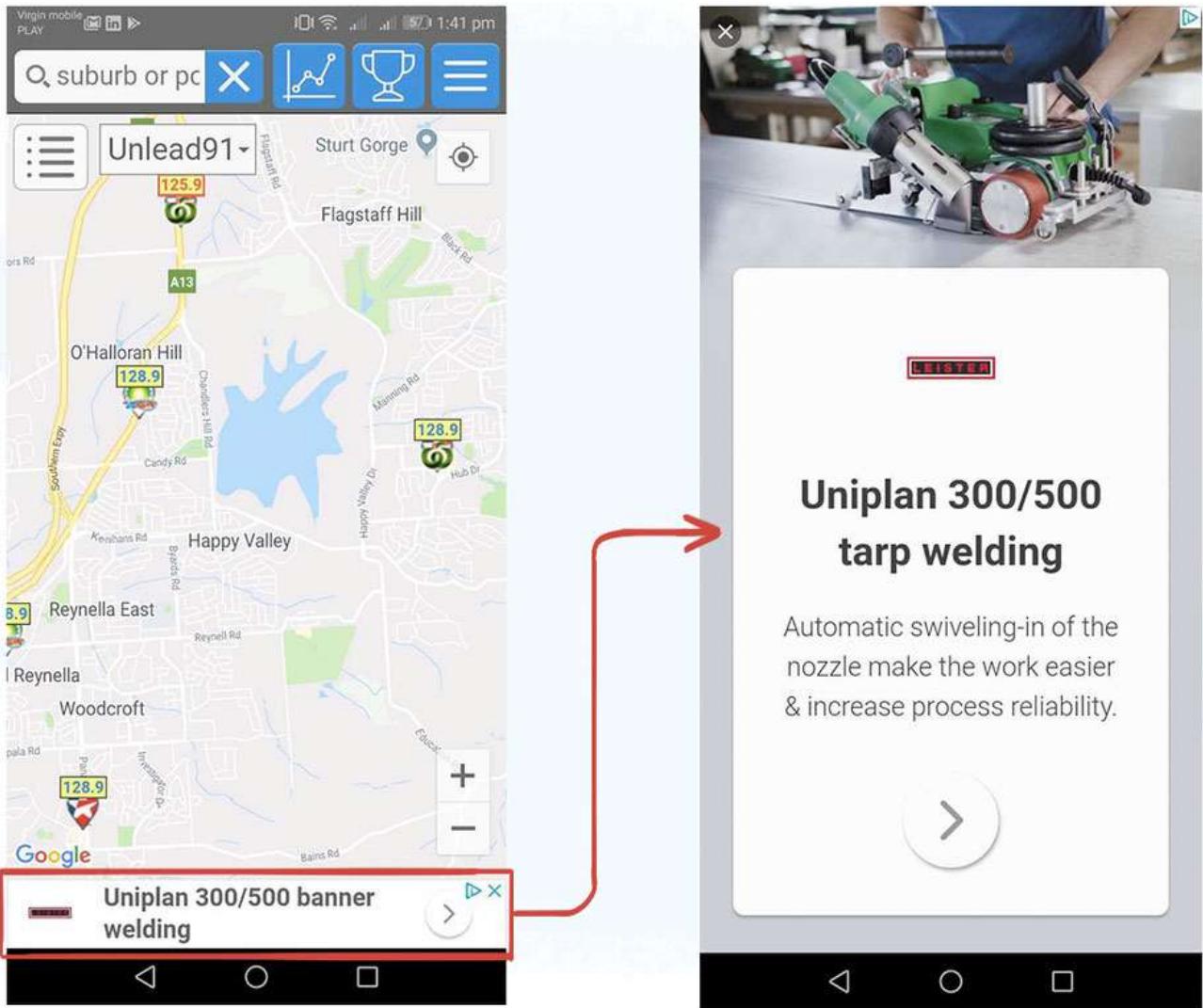
Source: dictionary.cambridge.org

Mobile App Advertising

Mobile app (aka in-app mobile) advertising relates to displaying ads inside mobile apps on smartphones and tablets.

Unlike web advertising on mobile devices that uses a browser to display ads, mobile apps need to use a software-development kit (SDK) to display ads.

The mobile app's developers integrate the given AdTech vendor's SDK into their app, define the ad space where the ads will run, and then select the ad medium (e.g. text, image, native, and video) and the ad format (e.g. interstitial and banner).

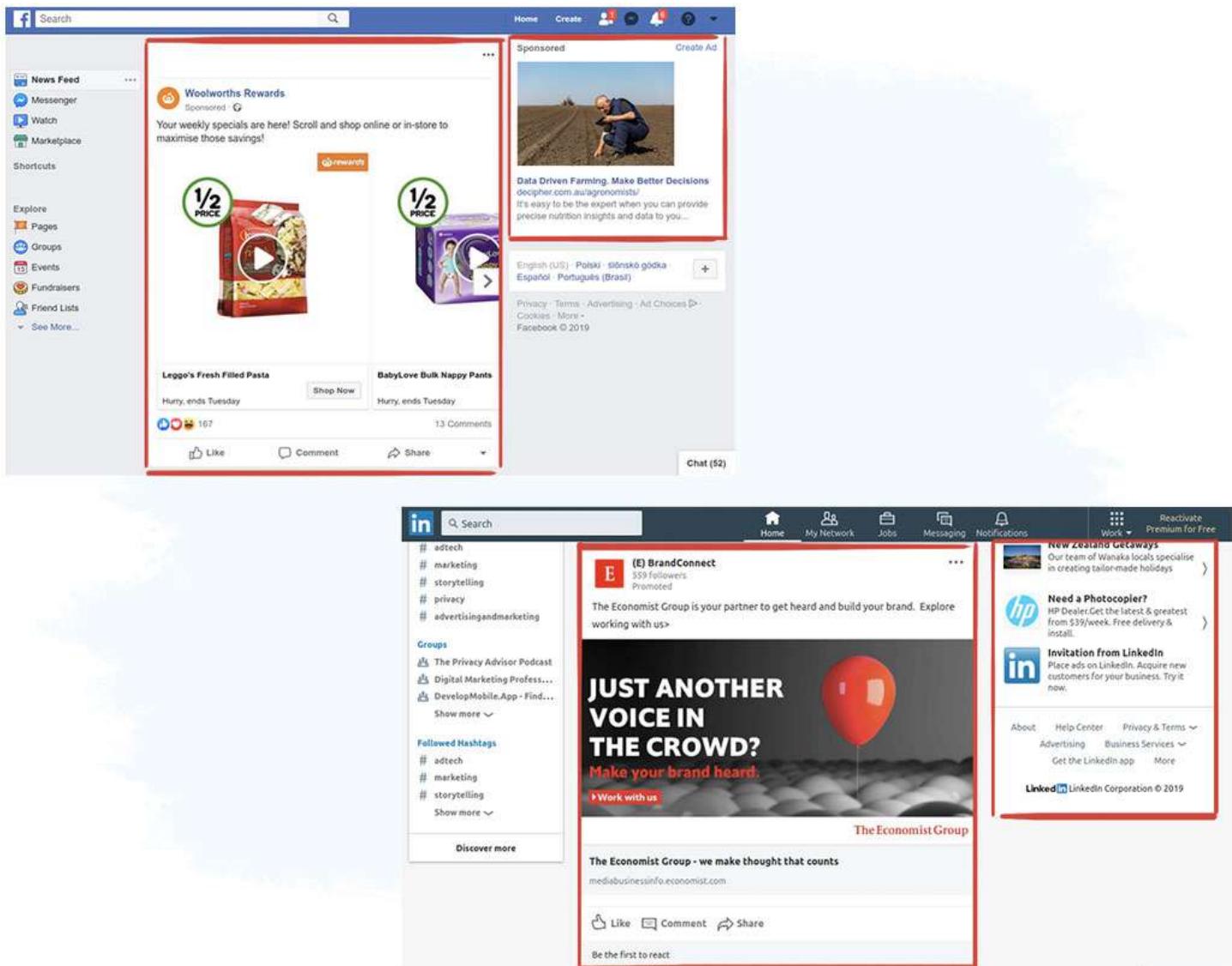


An example of an expanding image ad inside a mobile app.

Social Media Advertising

Although social media networks like Facebook, LinkedIn and Twitter fall into web advertising and mobile-app advertising categories, they are their own advertising channels.

Many popular social media sites like Facebook, Twitter, Pinterest, LinkedIn and Instagram utilize native advertising, where the ads appear in and next to the news feed, making them look like organic content:



Examples of social media advertising.

Advertising on social media platforms provides brands, advertisers and agencies with a number of advantages:

- Advertisers can retarget users using the email address they provided to a brand, which often results in high conversions.
- Some social media platforms, such as Facebook and LinkedIn, collect detailed demographic and behavioral data – including a person's name, age, location, interests, and education – providing brands with powerful audience-targeting capabilities.
- Compared to other advertising channels, such as display or video, social media advertising can be more cost-effective in terms of both reach and conversions.
- Because most ads that run within social media platforms are native ads, they often receive more engagement (viewable impressions, clicks, likes, etc.) than traditional banner ads and are less susceptible to ad-blocking software.

Advanced TV Advertising (OTT, Connected TV, and Addressable TV)

TV advertising has long been the cornerstone of many brands and agencies. The ability to reach a large audience with an engaging and often entertaining message helps increase brand awareness and drive sales.

Even though traditional TV is still alive and well, new forms of TV are starting to form, bringing with them new opportunities and benefits for brands and agencies.

These new forms of TV include:

Advanced TV: A term coined by the IAB referring to any form of TV other than the traditional broadcast, cable and satellite connections.

OTT: Over-the-top (OTT) refers to devices or services used to stream digital content to a connected TV.

Examples of OTT services include:

- Netflix
- Hulu
- HBO GO
- Amazon Prime
- Disney+
- AppleTV+
- Roku
- ZEE5

Connected TV: Connected TV (CTV) refers to devices that connect to the Internet and allow viewers to watch video content from over-the-top streaming services. Examples of CTV include smartTVs, gaming consoles, and streaming devices. The IAB Tech Lab doesn't consider desktop computers, laptops, smartphones, and tablets as examples of CTV.

Addressable TV: Unlike traditional linear TV advertising that shows the same ads during a given program, addressable TV aims to display different ads to different viewers during the same program.

It is able to achieve this by using data collected via Internet Protocol TV (IPTV), which includes connected TVs and OTT devices and services, and set-top boxes.

For example, a person living in Seattle watching *Mad Men* would see a different ad than a person living in Portland who is also watching *Mad Men*.

All of the above offer a number of new advantages for advertisers that are unattainable with traditional TV, such as targeting, attribution and measurement.

However, due to numerous technological barriers, the industry is still a few years away from delivering these new advantages at scale and with high accuracy.

DOOH Advertising

Out-of-home (OOH) advertising was a popular medium prior to the internet. Brands and agencies would advertise on billboards, street furniture (think bus stops and telephone boxes), and on taxis, buses and subway walls.



Source: JCDecaux



Source: JCDecaux

Thanks to technological advancements in OOH displays (e.g. digital screens, Internet connectivity and sensors) digital out-of-home (DOOH) advertising is giving new life to this traditional advertising medium and allowing brands and agencies to explore new creative formats.

Below are some examples that highlight the possibilities that DOOH has to offer:



Although DOOH is one of the most exciting trends in digital advertising, it is experiencing some initial hurdles around the media-buying process, attribution, measurement and targeting.

However, all of these areas present opportunities for AdTech companies and will likely be addressed and resolved in the coming years.

Search Advertising

Whenever you look for a product or service online, search engines like Google, Bing, and DuckDuckGo display a mix of organic and sponsored results. Search engines have ways to indicate which results are sponsored, and which are not.

Sponsored ads in Google search. Links are marked with a green "Ad" box.

Sponsored ads are displayed in the search engine when someone enters keywords matching the services or products offered by the advertiser. In this way, the ads perfectly match the query.

Search ads are considered to be very effective, as they are based on the explicit intent of the users, rather than just on implicit information about what they might be after, and are also displayed in the native ad format.

Both of these factors lead to higher click-through and conversion rates among search ads compared to banner ads.

Who Offers Search Ads?

Search engines

Most search-engine companies operate platforms allowing ads in their search results (Google does it via [AdWords](#), Bing does it via [Bing Ads](#), etc.). This is a natural way for search providers to monetize their huge user base.

While the [global search-engine market](#) is currently dominated by Google with an eye-watering 77% market share (and growing), there are many other search engines that make up the remaining percentage:

- [Google](#) (~77%)
- [Baidu](#) (~9%)
- [Microsoft Bing](#) (~8%)
- [Yahoo!](#) (~3%)
- [Yandex](#) (~1%)

Publishers

Although most Internet searches are carried out on one of the main search engines, many publishers (particularly ecommerce stores) have their own search functionalities and allow ads, often in the form of promoted listings.

The screenshot shows the Amazon search results for "smart watch". The top navigation bar includes "All", a search bar with "smart watch", a magnifying glass icon, "EN Hello, Sign in Account & Lists", "Orders", and a shopping cart icon. Below the search bar, there are links for "Deliver to Poland", "Today's Deals", "Help", "Registry", "Gift Cards", "Sell", and "Your Amazon.com". A banner at the top right says "Shop 12 Days of Deals". The search results start with a "Department" sidebar listing categories like Electronics, Smartwatches, Wearable Technology, GPS Trackers, Men's Fashion, Women's Fashion, Cell Phones & Accessories, Health & Household, and more. The main content area features a "GARMIN" advertisement for the fenix 5 Plus Series. It includes three smartwatches: a black model, a brown leather model, and a white model. Each is labeled "Limited time Deal" and has a price of \$559.95 (prime). Below the ad, there's a note about price variation and a sponsored product listing for a "Smart Watch, Bluetooth Smartwatch Touch Screen Wrist Watch with Camera/SIM Card Slot, Waterproof Smart Watch Sports Fitness Tracker Android Phone Watch Compatible with Android Phones Samsung Huawei". This product has a price of \$29.98 and 468 reviews. The bottom of the page shows filters for "Avg. Customer Review" (4 stars and up, 4.5 stars and up, 5 stars and up) and "Brand" (Samsung, LG).

The search functionalities on these sites not only make finding products and services easier, but also enable the publisher to offer search advertising to merchants.

This is a win-win situation for both the ecommerce store and the merchant (advertisers), as the ecommerce store is able to create a new revenue stream and the merchant is able to increase sales.

Now that we've examined the digital advertising mediums and channels, it's time to look at how these ads are served and displayed to users.

06. Ad Serving



Since the beginning of online advertising over two decades ago, a number of technologies have been introduced to solve the numerous problems advertisers and publishers face and to improve the entire media-buying and selling process.

While the invention of AdTech platforms like demand-side platforms (DSPs), supply-side platforms (SSPs), and ad exchanges helped shape the online advertising ecosystem, it's hard to look past one early piece of AdTech that is still relevant today — **the ad server**.

Ad servers have constantly evolved to meet the demands of advertisers and publishers and adapt to the rapidly changing field. As a result, many of the functionalities—e.g. targeting, budget control and frequency capping—appear in many of the more recent platforms, such as DSPs and SSPs.

In this chapter, we explore one of the most fundamental technology platforms and processes in online display advertising today.

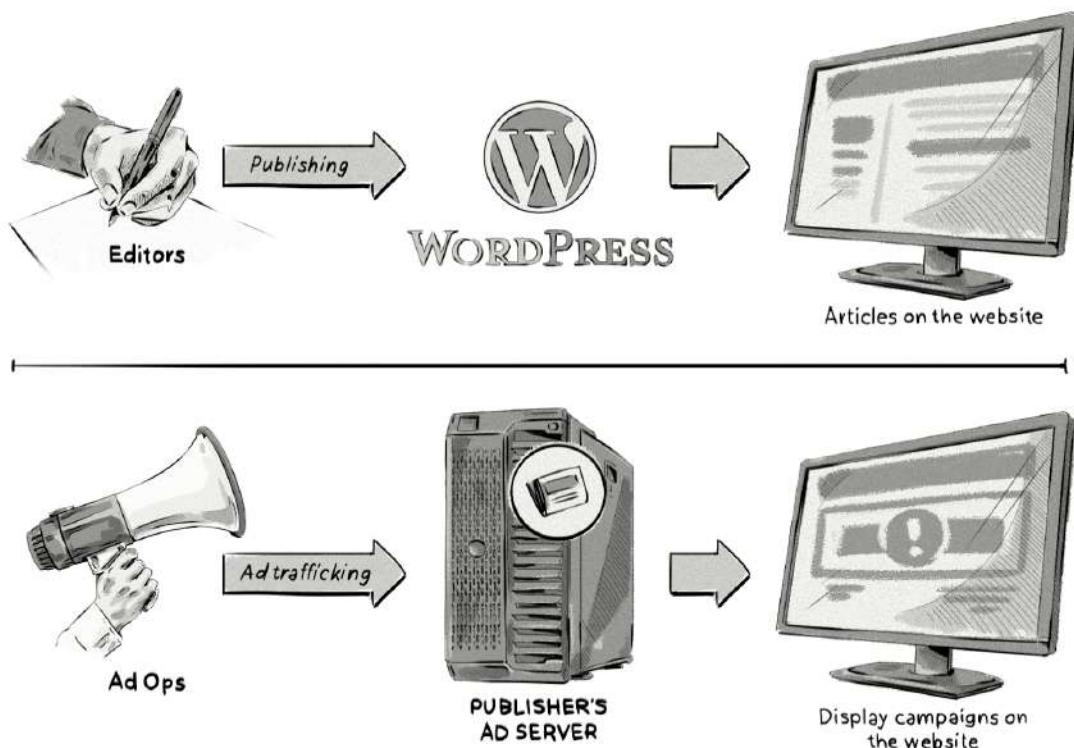
You'll not only learn about an ad server (platform) and ad serving (process) and how they work, but also uncover their inner workings and why they are a vital component of online display advertising.

What Is an Ad Server?

An **ad server** is an AdTech platform responsible for making decisions about what ads to show, serving them, and collecting and reporting data on impressions, clicks, etc.

To help you understand the role of an ad server, think of it this way:

Ad servers are to ads (creatives) what WordPress is to content (articles).



In the same way that WordPress is used to manage a website's content, ad servers are used to manage and display advertising on a website.

Publishers, advertisers and ad agencies use ad servers to run multiple campaigns, often by connecting to other AdTech platforms, such as demand-side platforms and supply-side platforms.

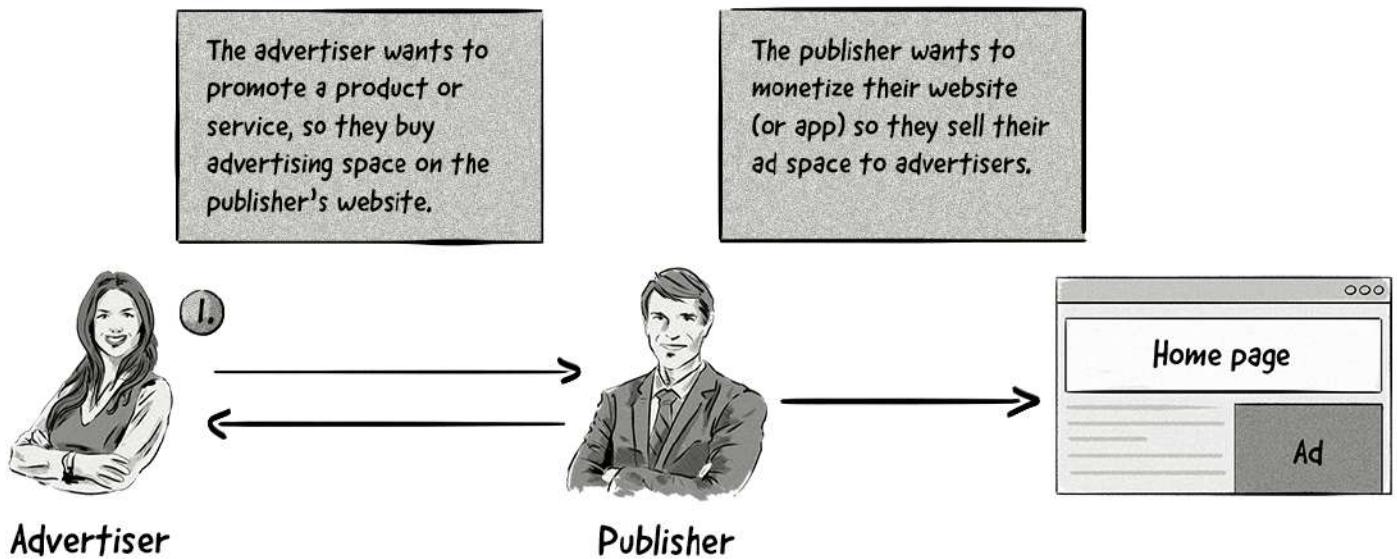
Campaign Execution Using an Ad Server: Then and Now

The way online ads have been bought, sold, and delivered has changed a lot over the past two decades, but what hasn't changed is the importance and role that ad servers play.

Below is an illustration of how the ad-serving process looked in the late 1990s to early 2000s, and how ad servers emerged.

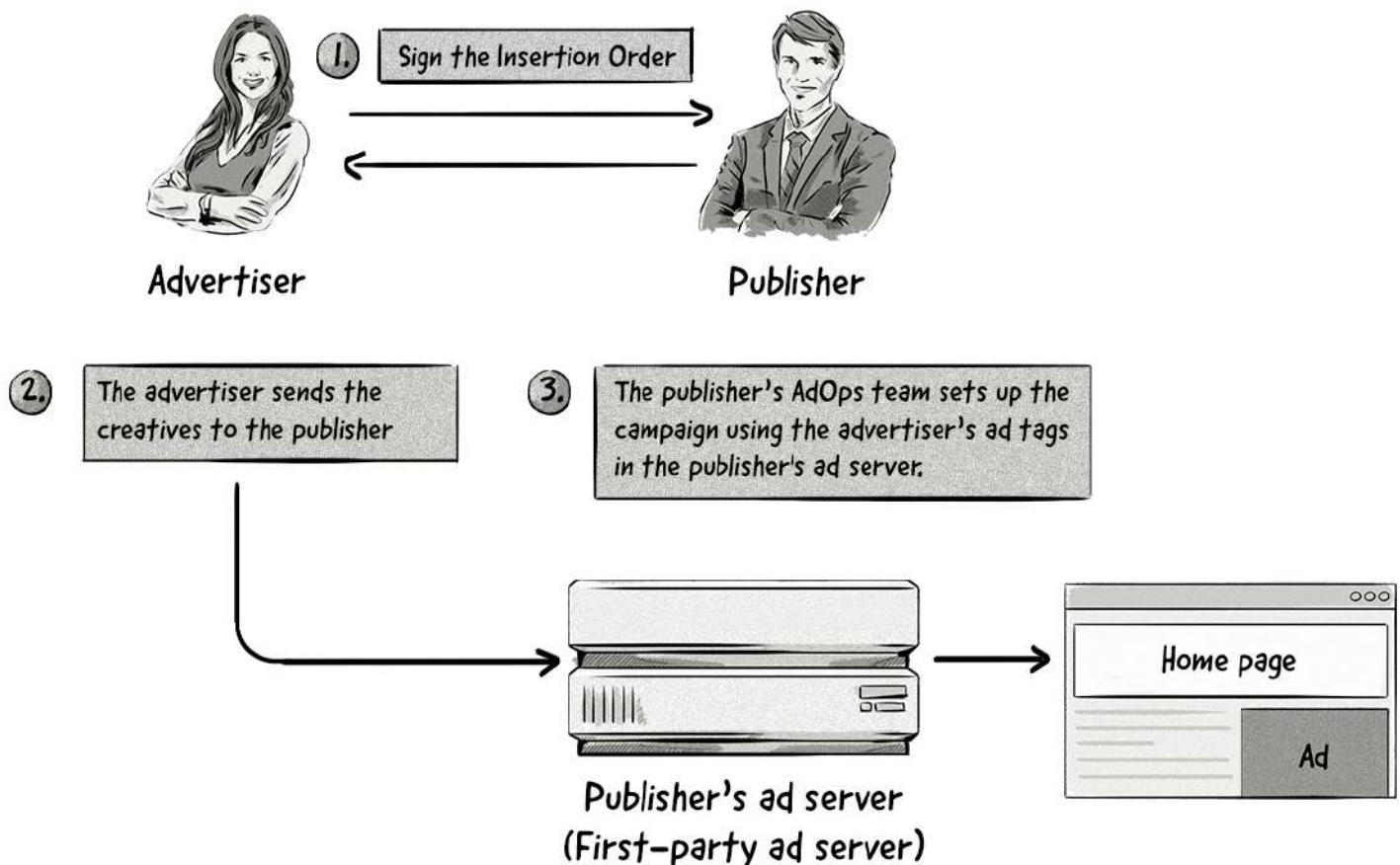
In the early days of online advertising, executing a campaign was a manual process that only involved direct communication between the advertiser and publisher.

The Advertiser-Publisher Relationship



Then, the publisher's ad server was introduced to help them run and report on advertisers' campaigns.

First-party (publisher's) ad servers are introduced



Here's how the basic flow would look:

1. The advertiser and publisher sign an insertion order (IO), which is a document (often a contract) that outlines the terms of the campaign, including flight dates (start and end dates), placement, ad format and size, pricing model (e.g. CPM or CPC), and a few other details.
2. The advertiser sends over a list (typically a spreadsheet) of its creatives.
3. The publisher's AdOps team sets up the campaign in its ad server.
4. Once the campaign starts, the advertiser then receives ongoing reports from the publisher about the performance of its campaign, such as impressions and clicks.

What's the Difference Between Ad Trafficking and AdOps?

The terms *ad trafficking* and *AdOps* are often confused with one another, but there is a small difference.

Ad trafficking is the name given to the process of setting up, monitoring, and optimizing the campaigns conducted by ad servers and/or other AdTech platforms.

AdOps are people who are responsible for setting up, monitoring, and optimizing campaigns.

In short, AdOps refers to the people and ad trafficking refers to the process.

First-Party (Publisher's) Ad Server

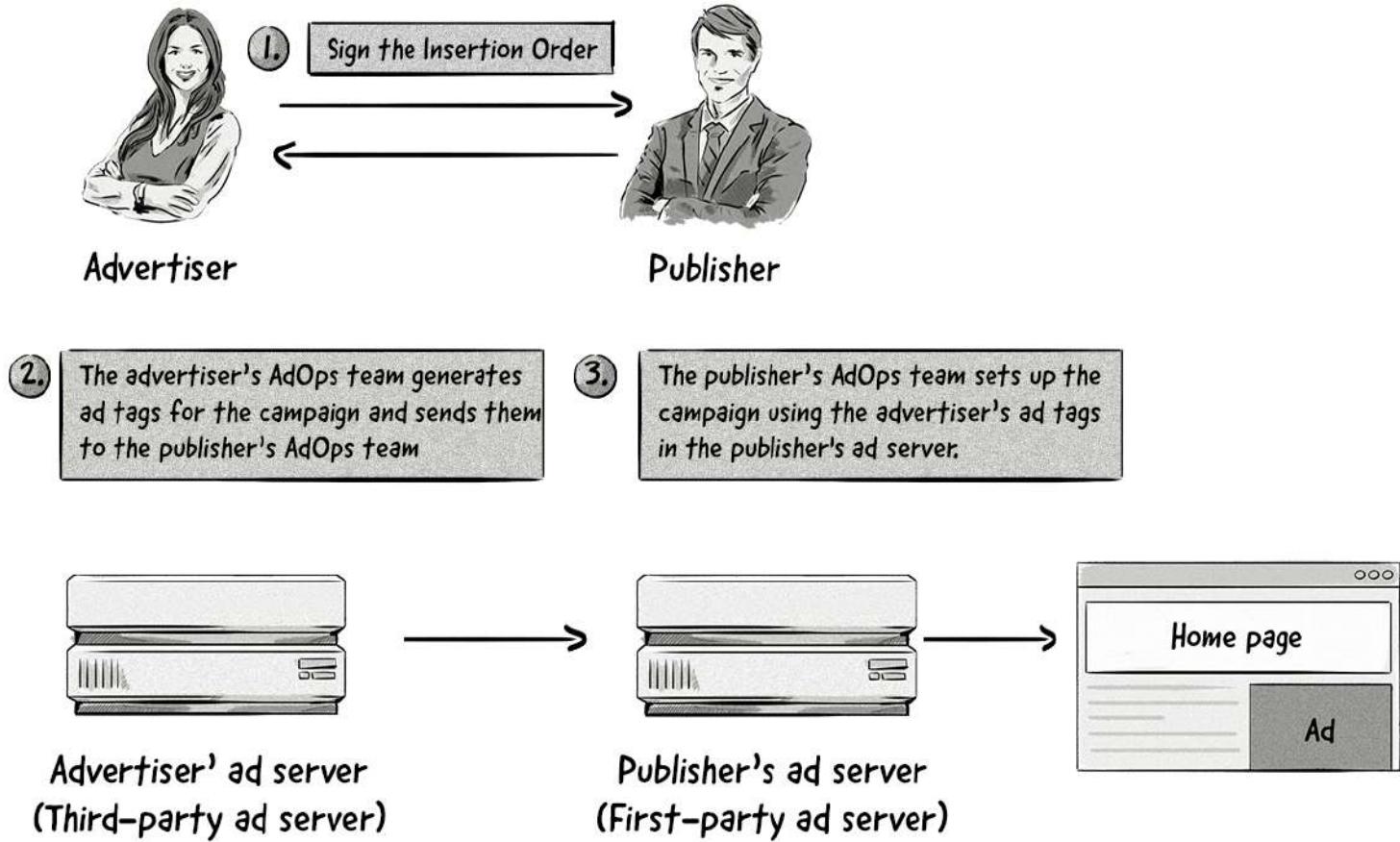
A publisher's ad server is tasked with filling the ad slots on a website by matching ads from direct campaigns, real-time bidding (RTB) auctions, and other media-buying processes.

They do this by making decisions about which ads to show on a website based on the targeting parameters of campaigns set up by advertisers, serving those ads, and reporting on their performance.

Another feature of ad servers is inventory forecasting, which involves predicting how much inventory a publisher will have available in the future and the performance of ad campaigns based on current and historical data.

Soon, advertisers started using ad servers to measure the performance of their campaigns for themselves. These ad servers are known as a third-party or advertiser's ad server.

Third-party (advertiser's) ad servers are introduced



Third-Party Ad Servers

Earlier in the book, we outlined the following challenges advertisers faced when dealing directly with publishers:

- Limited reach of a single campaign.
- Reporting overhaul – i.e. no single way to measure the campaign across different publishers.
- Reporting verification – i.e. no way to verify the reports provided by the publisher.

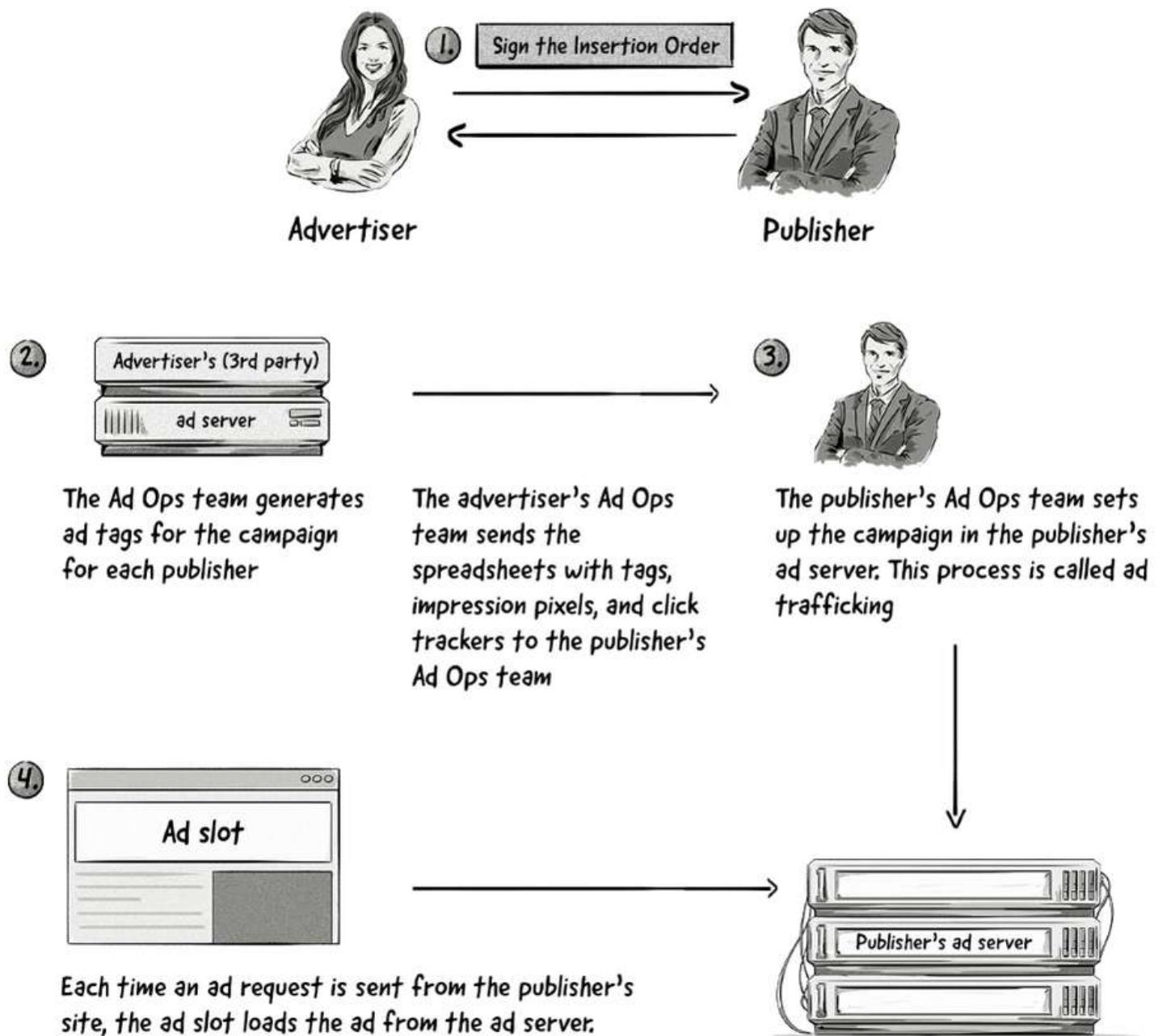
Even though the invention of the ad server solved many of these challenges through automation, new challenges arose for advertisers.

The booming online ad business was attracting more new publishers; however, not all of them were playing fair. Advertisers soon found that they could no longer trust the reports generated by publishers and ad networks.

In order to gain the independent reports from their campaigns that ran on multiple publishers and ad networks, advertisers started using independent ad servers, known now as third-party ad servers (aka advertiser's ad server).

An ad server allows advertisers to:

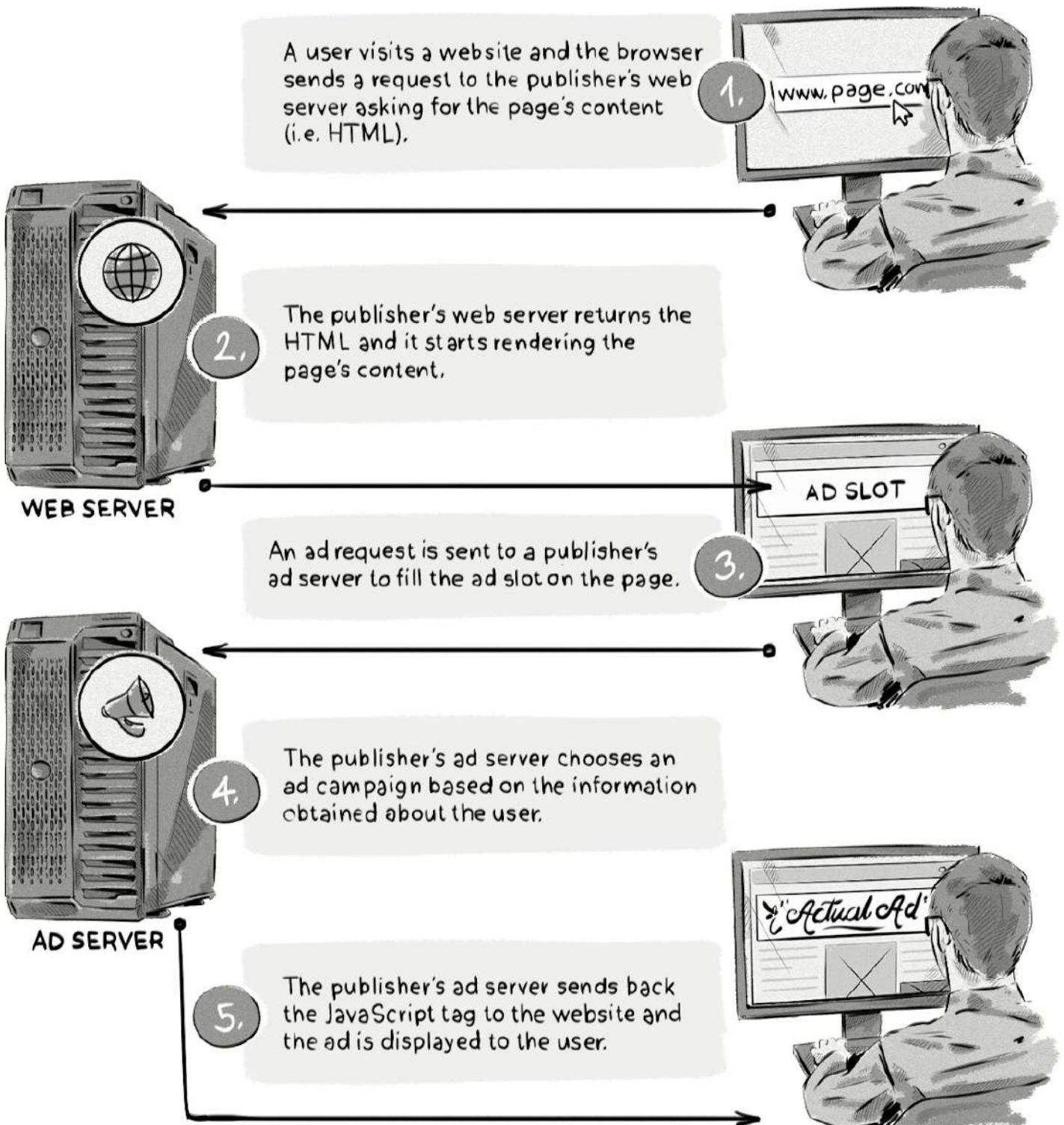
- Track the performance (impressions, clicks, conversions, etc.) of the whole campaign across all publishers in a single system.
- Measure the reach of a campaign while taking into account the co-viewership across publishers.
- Verify the reports provided by the publishers.



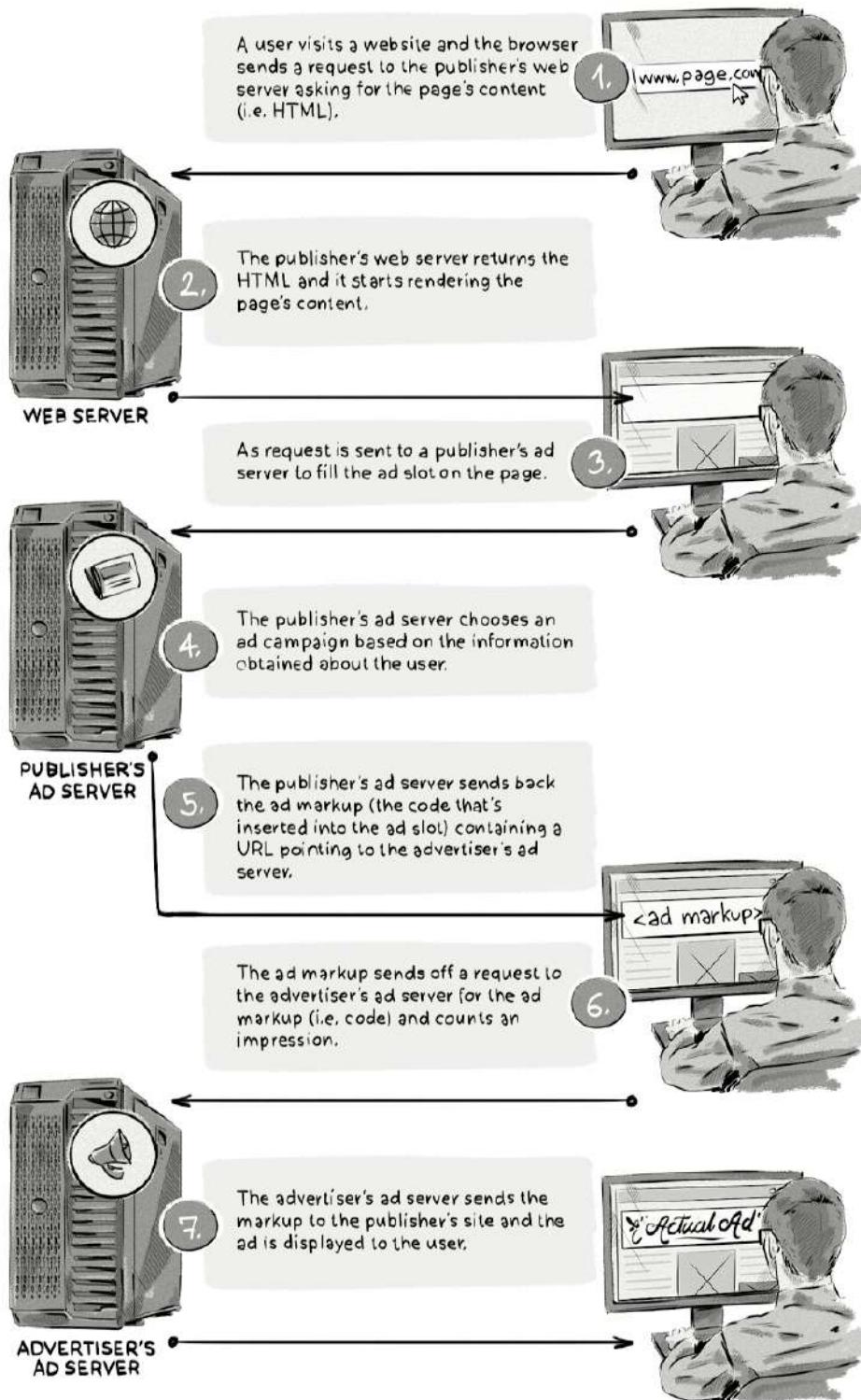
How Does an Ad Server Work?

Now that we know what an ad server is and what it is responsible for, let's take a look at its mechanics.

First, let's look at how a publisher's ad server works:



And now an advertiser's ad server:



First-Party vs. Third-Party Ad Servers: A Simple Comparison

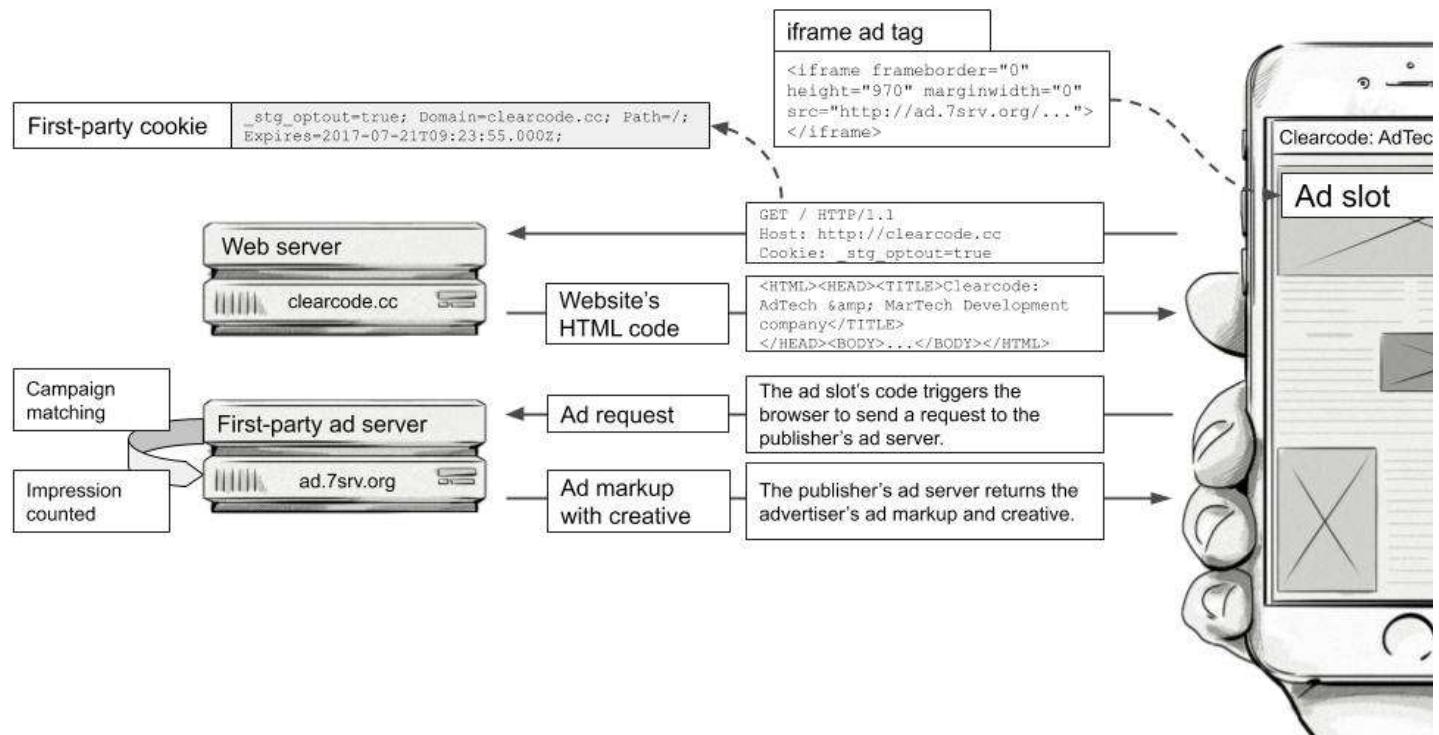
While first-party and third-party ad servers are essentially the same type of machine, they fulfill different responsibilities for publishers and advertisers.

First-Party Ad Server (Publisher's Ad Server)	Third-Party Ad Server (Advertiser's Ad Server)
Allows AdOps to manage ad slots on the website, run multiple direct campaigns (i.e. direct deals between the publisher and advertiser) and manage third-party tags from other ad servers or ad platforms, such as SSPs.	Tracks the performance of the campaigns across all the sites that are involved in a particular campaign (e.g. reach, impressions, clicks, conversions), calculates the return on investment (ROI) and attributes the conversions to the right publishers.
Helps publishers manage and predict their inventory fill rates across many advertisers, provides reporting for billing purposes and tracks their earnings and actual fill rates. A first-party ad server also identifies the efficiency of third-party demand sources (e.g. via RTB) and direct deals, which helps publishers identify which sources are buying the most ad space and assign priority accordingly.	Helps the advertiser optimize its future media buys based on past data, identifies which sites and targeting criteria worked and which didn't, and run A/B tests to determine which ads deliver the best performance.
Allows publishers to forecast the amount of inventory that match certain targeting criteria. For example, it can tell them how much traffic they receive from NY State on their homepage's ad placement so that the sales team can offer the right quantity on insertion orders for advertisers.	Allows advertisers to audit and verify the numbers (i.e. performance metrics) for billing purposes.

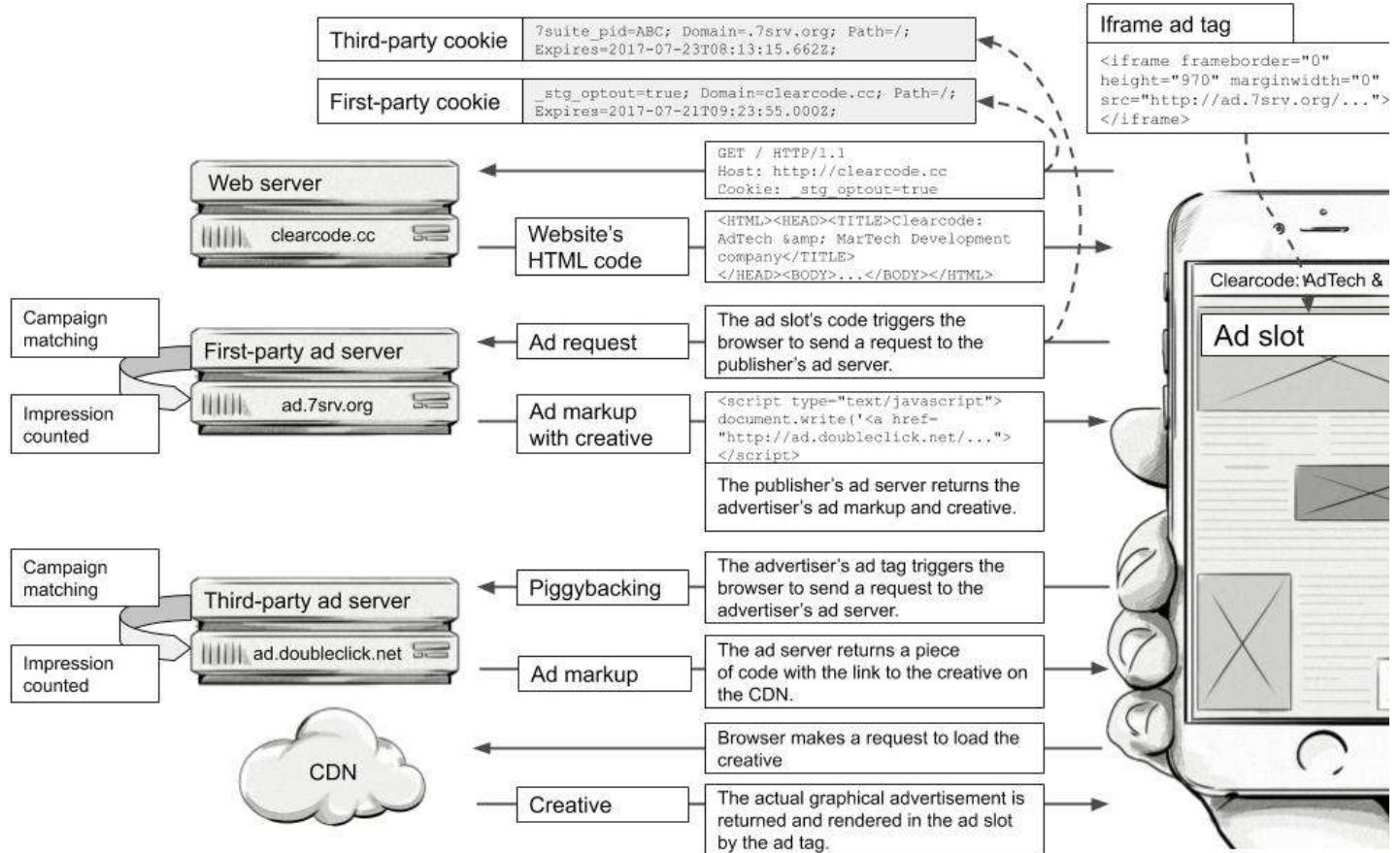
How Ad Serving Works From a Technical Perspective

Below are two detailed technical examples of how ad serving works.

The first illustrates how ad serving works with just a publisher's ad server:



The second illustrates the ad-serving process with both a publisher's and an advertiser's ad server:



The Anatomy of an Ad Server

Below you'll find the various ad-serving components, such as the ones listed in the diagrams above.

Ad Tags

An ad tag is a piece of code that is inserted into an ad slot in order to display an ad.

There are different types of ad tags depending on their implementation.

Below, we list the most common ad tags, how they are used and implemented, and the advantages and disadvantages they offer:

JavaScript Ad Tags

Usage: For rendering display ads on web pages via a desktop or mobile browser. JavaScript ad tags are also used for display ads in mobile apps, but generally these will be custom tags or Mobile Rich Media Ad Interface Definition (MRAID).

Implementation: JavaScript ad tags are placed directly in the publisher's page code.

Advantages:

- Ads can interact with a publisher's website
- Viewability can be tracked
- Ads can be loaded at the same time or after the content is loaded (depends on the implementation)

Disadvantages:

- Ads can change the content of the publisher's website, causing it to break its functionality.
- Ads could compromise the security of the website and result in installing malware that captures sensitive data from forms, such as usernames, passwords, email addresses, etc. An example of this is the recent [Magecart attack](#) where credit-card details of a possible 380,000 customers were taken from Newegg and British Airways via JavaScript injection.

```
<script type="text/javascript"><!--
google_ad_client = "pub-11111111";
/* 160x600 - TOP */
google_ad_slot = "12345";
google_ad_width = 160;
google_ad_height = 600;
//-->
</script>
<script type="text/javascript"
src="http://pagead2.googlesyndication.com/pagead/show\_ads.js">
</script>
```

An example of a JavaScript ad tag.

Iframe Ad Tags

Usage: For rendering display ads on web pages via a desktop or mobile browser.

Implementation: Iframe ad tags are HTML tags that are added to a publisher's page code. The iframe completely isolates the code loaded in the iframe, and therefore, prevents it from interacting with the rest of the content of the website.

Advantages:

- Protects the publisher against ad codes that could change the content of the website.

- Increases security by isolating JavaScript code in the iframe so that it cannot interact with elements on the website.
- Ads load after the contents of the website, which helps decrease the time it takes to load the contents of the page.

Disadvantages:

- Limited interaction with a publisher's website – i.e. it requires additional JavaScript code to be installed on the publisher's website to implement expandable ads.
- Can't reliably track the viewability of ads.

Here's an example of an iframe ad tag from [OpenX](#):

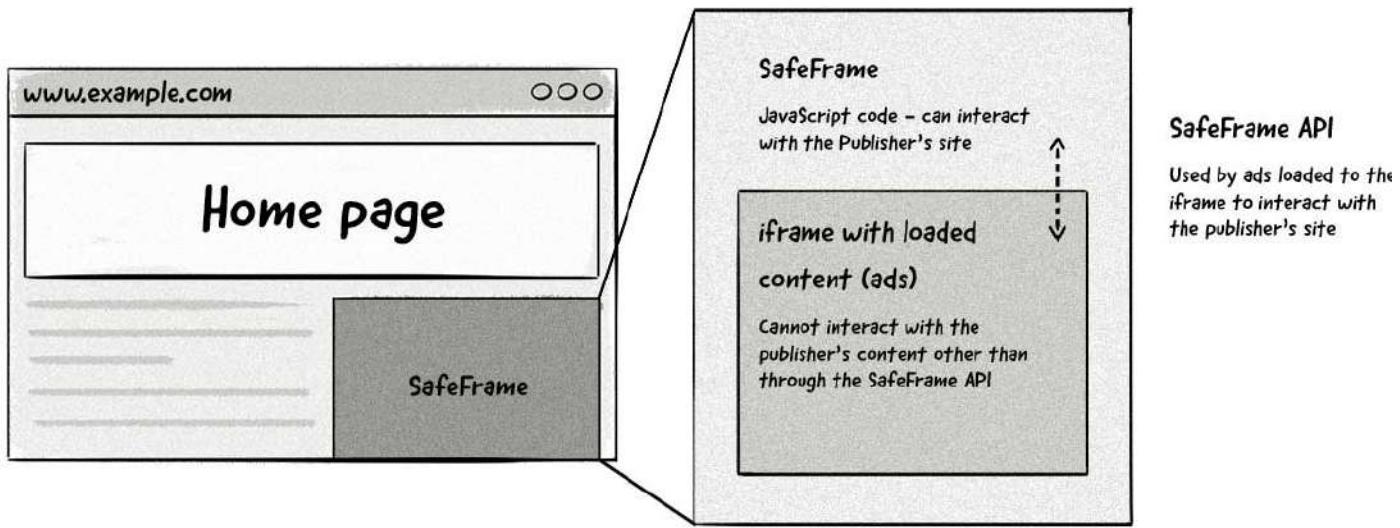
```
<iframe id='a62ae7d3' name='a62ae7d3'
src='http://delivery_server_domain/w/1.0/afr?auid=8635&cb=INSERT_RANDOM_NUMBER_HERE&rd=5&rm=3"
frameborder='0' scrolling='no' width='728' height='90'>
<a href='http://delivery_server_domain/w/1.0/rc?cs=acd22faf&cb=INSERT_RANDOM_NUMBER_HERE"
target='_blank'>
<img
src='http://delivery_server_domain/w/1.0/ai?uid=8635&cs=acd22faf&cb=INSERT_RANDOM_NUMBER_HERE"
border='0' alt=''/></a></iframe>
```

SafeFrame

In order to solve the issues related to both JavaScript ad tags and iframe ad tags, a new standard was introduced – **SafeFrame**.

SafeFrame is an Interactive Advertising Bureau (IAB) standard that combines the advantages of iframe and JavaScript tags and eliminates many of their disadvantages.

The SafeFrame ad slots are implemented in JavaScript with an API that loads the actual ads in iframes, but allows them to interact with its API to expand the content or track viewability. At the same time, it protects the publisher's site from unwanted changes and prevents visitors' sensitive information from being collected.



Here's how the SafeFrame implementation works:

1. The user accesses the publisher's website and the browser sends a request to the publisher's web server to fetch the content and SafeFrame ad markup.
2. SafeFrame (JavaScript) loads an iframe with the SafeFrame API, allowing it to interact with the publisher's site.
3. The ad is rendered and shown to the user.
4. At the same time, data is collected by viewability and measurement vendors to provide advertisers with reports.

It's important to note that the ad in the iframe loaded by the SafeFrame is isolated – i.e. third-party ad servers can run any JavaScript code inside the iframe, but it won't affect the publisher's website. Only specific sets of instructions and interactions with a publisher's site are allowed via the SafeFrame API, such as data collection for viewability and measurement.

VAST and VPAID (For Video Ads)

When it comes to serving video ads, the video ad-serving template (VAST) and video player ad-serving interface definition (VPAID) formats are used.

VAST is an XML schema developed by the IAB. It enables in-stream video ads (i.e. ads are displayed in the video player, like on YouTube) served from video ad servers and played in video players on a number of publisher sites and on different devices (e.g. desktop, mobile, tablet, etc.).

VPAID is a piece of JavaScript that enables video ad units and video players to interact with one another.

IMG Ad Tags

IMG ad tags are HTML tags and are similar to iframe tags.

Usage: These ad tags are mainly used to display ads in mobile apps and in the <noscript> section of other types of ad tags, which are used as fallbacks when the browser does not support or execute JavaScript.

Implementation:

Most AdTech platforms and publishers will only accept snippets of HTML/IMG ad tags and not full HTML code (e.g. no <html>, <head> or <title> tags).

See example of an HTML/IMG ad tag below:

```
<a href="https://www.clearcode.cc/">  </a>
```

Advantages:

- HTML/IMG ad tags are simple in structure and format, meaning they can be displayed in web browsers and apps without facing too many technical issues.
- They can utilize a content-delivery network (CDN) to reduce the time it takes the browser to load them, increasing the chances of the visitor seeing the ad.

Disadvantages:

- HTML/IMG ad tags can't display rich media ads (e.g. expandable or interactive ads).

Spreadsheets with ad tags

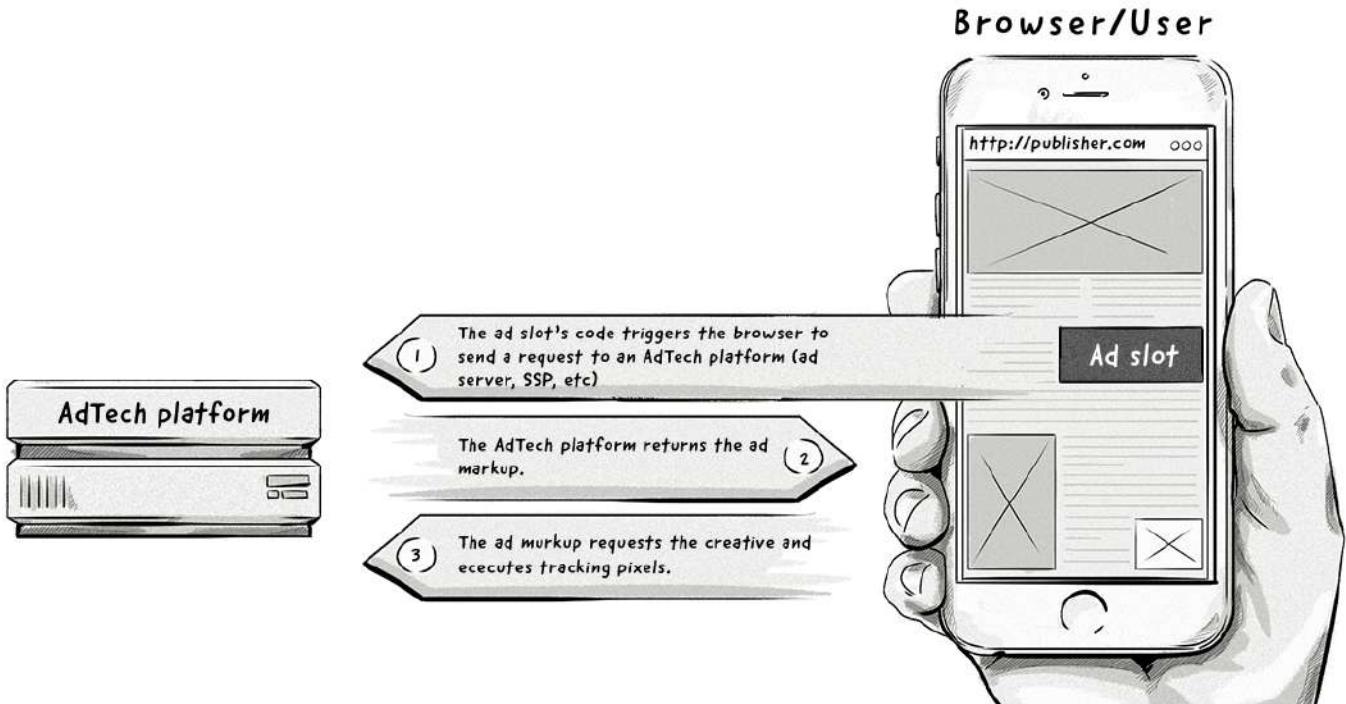
In order for advertisers to keep track of ad tags used in their campaigns, they often create spreadsheets.

A typical spreadsheet will include the list of placements and the respective ad tags. Even though this is a manual and error-prone process, it is still the most common way of trafficking the non-programmatic display campaigns (i.e. direct deals between a publisher and advertiser) and also some programmatic campaigns when using self-serve AdTech platforms.

Placement ID	Site	Placement Name	Placement Type	Size	Start Date	End Date	Standard Tag	Frames/JavaScript	Internal Redirect To	JavaScript Tag	Instructions	Creative QA
105492041	kanary.co	K-Kanary-web-180x150-Date	In-Page	180x150	17/12/13	25/01/14		<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.5.sz=180x150.cnt=1&stamp=?> WID=180x150.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.5.sz=180x150.cnt=1&stamp=?> WID=180x150.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.5.sz=180x150.cnt=1&stamp=?> WID=180x150.hdr=1</script>		TRUE
105492042	kanary.co	K-Kanary-web-180x90-Date	In-Page	180x90	17/12/13	25/01/14	"	<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.6.sz=180x90.cnt=1&stamp=?> WID=180x90.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.6.sz=180x90.cnt=1&stamp=?> WID=180x90.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.6.sz=180x90.cnt=1&stamp=?> WID=180x90.hdr=1</script>		TRUE
105492102	kanary.co	K-Kanary-web-720x90-CG	In-Page	720x90	17/12/13	25/01/14	"	<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.10.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.10.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.10.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1</script>		TRUE
105492098	kanary.co	K-Kanary-web-300x60-CG	In-Page	300x60	17/12/13	25/01/14	"	<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.15.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.15.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.15.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1</script>		TRUE
105492127	kanary.co	K-Kanary-web-720x90-Date	In-Page	720x90	17/12/13	25/01/14	"	<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.19.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.19.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.19.sz=720x90.cnt=1&stamp=?> WID=720x90.hdr=1</script>		TRUE
105492121	kanary.co	K-Kanary-mobile-300x60-Date	In-Page	300x60	17/12/13	25/01/14	"	<IFRAME SRC="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.18.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1"	Image URL (USE THIS TAG IN DFP ONLY): https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.18.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1	<SCRIPT>language="JavaScript1.1" src="https://ad.doubleclick.net/clk/nw/imp/N9818.18.185388.KAN/33688.KANARY.CO/B79/72188.18.sz=300x60.cnt=1&stamp=?> WID=300x60.hdr=1</script>		TRUE

Ad Markup

Ad markup is a piece of code that's retrieved from an ad server or some other AdTech platform via an ad tag and rendered in an ad slot.



Ad markup is responsible for two main activities:

1. Loading the actual creative file into the ad slot.
2. Tracking the impression by loading tracking tags (pixels) for measurement, ad verification, viewability, etc.

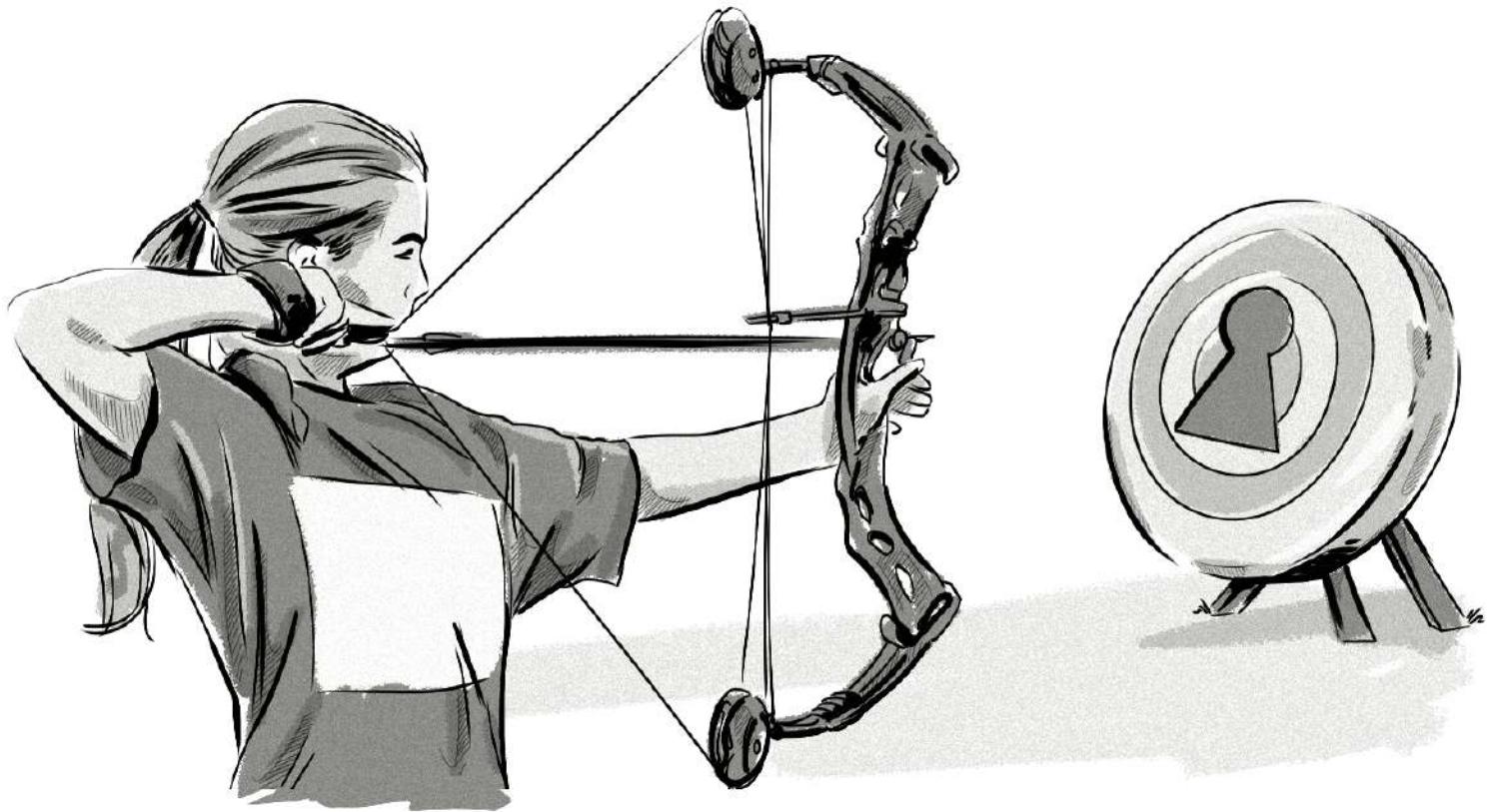
```
<a href="http://landingpage.com/"></a>
```

An example of simple ad markup.

Chapter Summary

- Ad serving is one of the fundamental processes in online advertising.
- A first-party ad server is used by publishers to manage the ad slots on their websites, serve ads from direct campaigns, manage other campaigns (e.g. real-time bidding), and report on the performance of the ads (e.g. impressions and clicks).
- A third-party ad server is used by advertisers to manage their creatives, send ads to publishers, and collect data about the performance of their campaigns.

07. Ad Targeting and Budget Control



In the context of online advertising, targeting relates to displaying ads to users who match a series of criteria.

For example, let's imagine an advertiser who sells gardening products has identified that its target audience consists of people between the ages of 30 and 50 and who live in rural areas of the US. The advertiser would then want to display its ads to people who match those criteria.

When it comes to direct deals between an advertiser and publisher, targeting was traditionally carried out by ad servers, whereby an advertiser would define the targeting criteria in the insertion order – e.g. state which pages and sections of a publisher's site to show its ads on.

The publisher's AdOps team would then configure the advertiser's targeting criteria in its ad server (first-party ad server).

Even though targeting is still carried out via ad servers, many other AdTech platforms (e.g. demand-side platforms and supply-side platforms) now offer targeting capabilities.

In this chapter, we'll talk about targeting in the context of ad servers.

By setting targeting criteria for a campaign, an advertiser can choose which web traffic is relevant for them.

Below are some examples of targeting methods in online advertising.

Contextual Targeting

Contextual targeting allows advertisers to display relevant ads based on the website's content rather than data about the visitor. This method of targeting is widely used in magazines and newspapers.

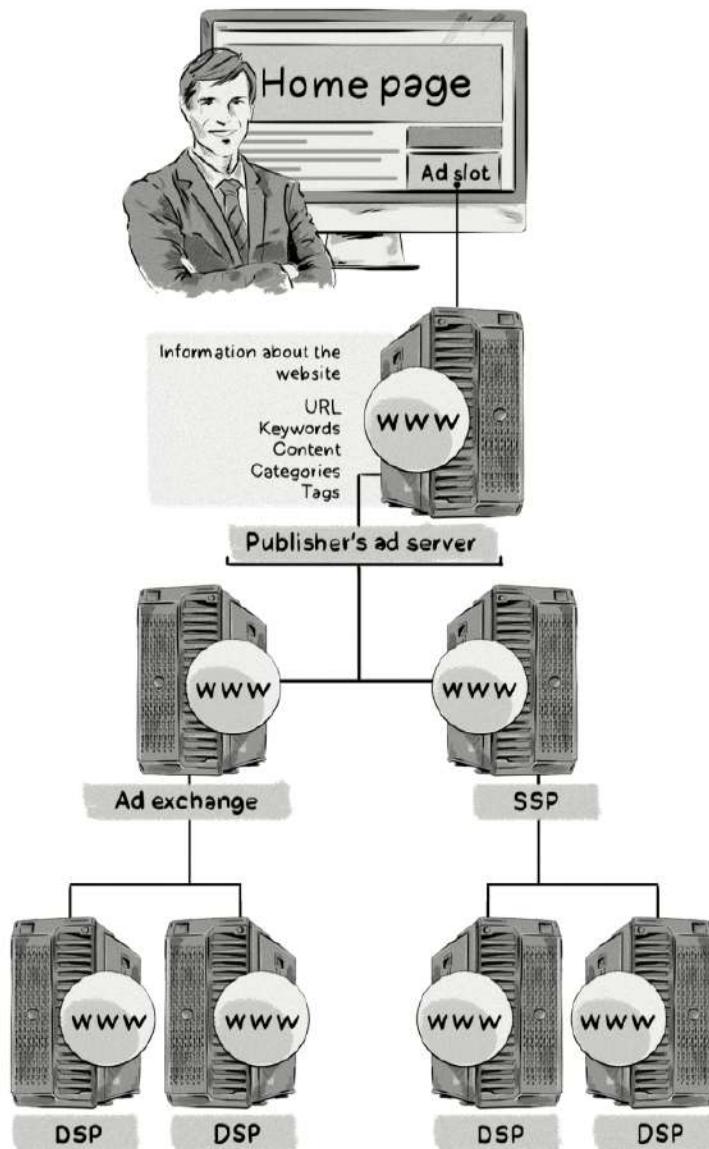
The screenshot shows the Expedia.com.au homepage with a search interface for flights and hotels. A promotional banner for Queensland, Australia, is displayed on the right side. The banner features the text "Queensland AUSTRALIA", "Find your perfect next island escape", and "20% off hotels!". It also includes a small note "*T&Cs apply." and a "BOOK NOW" button. The main search form includes fields for Origin and Destination cities, departure and return dates, room count, and guest details. Below the search form, there is a promotional message: "Save up to AU\$200 on Expedia packages Book Flight + Hotel at the same time*".

Contextual ads are a way to precisely target the ad without excessive need for personal data.

Many advertisers and publishers use contextual targeting, either in isolation or in combination with other targeting methods, because it's very effective for specific kinds of content.

How Does Contextual Targeting Work?

Contextual targeting



In contextual targeting, every element of the process uses information about the website and page to determine which ads to display.

A step-by-step explanation of how contextual targeting works:

1. A web crawler scans URLs and categorizes the content and ad placements.
2. When a visitor accesses a website, information associated with the URL is passed to the ad server via the ad request.
3. This ad request and the contextual information is passed on to other AdTech platforms, such as ad exchanges and supply-side platforms.
4. The ad exchanges and supply-side platforms relay this information to demand-side platforms, which then bid on the impression.
5. The winning DSP then sends the ad back to the publisher and displays the ad to the visitor.

Benefits of Contextual Targeting

Although contextual targeting may seem rather simple compared to other targeting methods, it provides advertisers and publishers with a number of benefits:

- Most contextual ads don't rely on personal data, helping advertisers and publishers reduce their exposure to privacy and data-protection regulations, like the GDPR.
- Contextual ads can offer safer brand protection.
- They have shown they can [increase purchase intent by 63%](#).
- They are found to be less unnerving than behaviorally targeted ads, while still being based on the interests of users – e.g. advertisers can show ads for smartphone plans to people reading articles about smartphones.

Keywords

Keywords are valuable targeting variables for advertisers as they provide an accurate picture of the type of content the website visitor is consuming.

There are a couple of ways an ad server can identify which keywords are on a given web page, such as via the tags used on the page by the editor that highlight the key topics covered in the content and via extracting the keywords found on the page, usually done either with JavaScript or server-side web crawling.

These keywords are then typically passed to the ad tag, so that the ad server receives them in the ad request and uses them in the decisioning process (when deciding which ad to serve).

So, for example, if an advertiser wants to display ads promoting a new smartphone plan, it would target visitors who read articles containing the keywords *smartphone*, *mobile phone*, etc.

Ad Slot and Ad Position

Advertisers may also want to display ads that are of a certain size or located in a specific area of a webpage – for example, ad slots that are 728×90 px and located at the top of the page.

Because this type of targeting is quite broad, it is usually combined with other targeting methods.

Publisher's URL

Targeting users based on the publisher's URL is very similar to the way advertisers target consumers in print media.

By displaying ads on specific websites, advertisers are able to reach a broad range of online consumers based on their interests, rather than based on their demographic information like age and gender.

There are two levels at which advertisers can target website visitors:

Domain

Advertisers can target audiences based on the publisher's domain name. However, this only applies in a direct advertiser-publisher relationship where the publisher owns many different websites.

This is often connected with run-on-site (ROS) targeting in ad networks, whereby advertisers show their ads on specific domains.

Section and URLs

The advertiser may choose to target certain sections of the site.

For example, if a site covers a lot of topics (like a news site), the advertiser may want to only target the technology section or entertainment section.

The problem is that usually these aren't clearly identified by just the URL and the publisher may need to pass the section name in the ad tag to enable the ad server to use this variable in its targeting.

This method of targeting is often connected with run-on-network (RON) targeting in ad networks, whereby advertisers show their ads on a specific group of websites.

IP and Geolocation

Geolocation targeting involves displaying ads to users based on their current location.

For example, if an online consumer was reading news articles on a laptop in Chicago, they could very well see ads promoting shops, restaurants and services in the Chicago area.

But how do advertisers know where consumers are located?

An ad server receives a request from the consumer's browser, which carries its IP address. The IP address is mapped to the specific location of the consumer using an external database, such as [MaxMind](#) or [Neustar](#), which maps the IP address to the country, region and city.

GeoIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization
209.95.50.164	US	New York, New York, United States, North America	10011	40.7308, -73.9975	500	WestHost	Hosting Services Inc

The image above is a query from MaxMind.

Native mobile apps can also pass the exact longitude and latitude from a smartphone's GPS to the ad server.

In such cases, the ad server is capable of targeting the users within a radius of a certain point (e.g. within five miles of a given point of sale). This makes geolocation targeting much more accurate and precise than the IP address method.

However, even GPS information can sometimes be inaccurate and even fraudulent.

To improve the accuracy of location data, some data companies collect, aggregate, and combine different data points and sensors.

Imagine this situation: A consumer is eating a sandwich on a bench in downtown New York and playing a game on their smartphone. Starbucks (i.e. the advertiser) could display an ad to that consumer encouraging them to visit the Starbucks cafe located five minutes down the road from the consumer's location.

Browser Type, Operating System and Device Type

Every ad request to the ad server carries a user-agent HTTP header, e.g.:

```
User-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36
This is Mac OS X 10.12.6 running Chrome 60.0.3112.101
```

In the example above, 14D27 identifies as an iPhone 7 Plus, and we see it's running iOS 10.2.1.

From this information, we can parse the operating system, browser type and version, and can detect the device type, brand and model (in the case of mobile devices, as shown above with the iPhone).

Targeting online consumers based on their hardware or software enables advertisers to reach a specific audience with a highly relevant message.

For example, a mobile-gaming company could display ads promoting its newly developed Android game to consumers using Android-powered smartphones and tablets.

IAB Content Taxonomy

The IAB provides a standard for the categorization of websites.

Advertisers are able to purchase digital ad space based on the categories supplied in the ad request, and can also choose not to show their ads on websites based on the categories.

Below is a shortened list of the taxonomy:

Unique ID	Tier 1	Tier 2	Tier 3
1	Automotive		
2	Automotive	Auto Body Style	
3	Automotive	Auto Body Style	Commercial Trucks
...
52	Business and Finance		
53	Business and Finance	Business	
54	Business and Finance	Business	Business Accounting & Finance
...
223	Healthy Living		
224	Healthy Living	Children's Health	
225	Healthy Living	Fitness and Exercise	Participant Sports
...
239	Hobbies & Interests		
255	Hobbies & Interests	Arts and Crafts	Photography
...
656	Travel	Travel Locations	Africa Travel
657	Travel	Travel Locations	Asia Travel
658	Travel	Travel Locations	Australia and Oceania Travel
...

The IAB Content Taxonomy contains over 30 Tier 1 categories and over 1,100 individual entries (rows).

Below is part of the IAB Content Taxonomy from the OpenRTB (version 2.4) specification, containing 390+ content categories:

```

1   {
2     "IAB1": "Arts & Entertainment",
3     "IAB1-1": "Books & Literature",
4     "IAB1-2": "Celebrity Fan/Gossip",
5     "IAB1-3": "Fine Art",
6     "IAB1-4": "Humor",
7     "IAB1-5": "Movies",
8     "IAB1-6": "Music",
9     "IAB1-7": "Television",
10    "IAB2": "Automotive",
11    "IAB2-1": "Auto Parts",
12    "IAB2-2": "Auto Repair",
13    "IAB2-3": "Buying/Selling Cars",
14    "IAB2-4": "Car Culture",
15    "IAB2-5": "Certified Pre-Owned",
16    "IAB2-6": "Convertible",
17    "IAB2-7": "Coupe",
18    "IAB2-8": "Crossover",
19    "IAB2-9": "Diesel",
20    "IAB2-10": "Electric Vehicle",
21    "IAB2-11": "Hatchback",
22    "IAB2-12": "Hybrid",
23    "IAB2-13": "Luxury",
24    "IAB2-14": "Minivan",
25    "IAB2-15": "Motorcycles",
26    "IAB2-16": "Off-Road Vehicles",
27    "IAB2-17": "Performance Vehicles",
28    "IAB2-18": "Pickup",
29    "IAB2-19": "Road-Side Assistance",
30    "IAB2-20": "Sedan",
31    "IAB2-21": "Trucks & Accessories",
32    "IAB2-22": "Vintage Cars",
33    "IAB2-23": "Wagon",
34    "IAB3": "Business",
35    "IAB3-1": "Advertising",
36    "IAB3-2": "Agriculture",
37    "IAB3-3": "Biotech/Biomedical",
38    "IAB3-4": "Business Software",
39    "IAB3-5": "Construction",
40    "IAB3-6": "Forestry",

```

Examples of some IAB content categories.

Source: [Github](#)

Day of Week and Time of Day

Displaying ads to consumers based on the day of the week and even time of day can allow advertisers to reach their desired audience at the right time, and also to avoid wasting their ad budget.

For example, an advertiser that works for a large pizza restaurant could advertise its Friday night specials on Friday afternoons between 3–8pm. This would work out to be especially beneficial if its ad was being displayed next to competitors that weren't offering any special promotions targeted for that particular day.

Similarly, if a brand notices that ad engagement is higher at certain times of day, then it could opt to display ads to its audiences at those times. Not only would the brand increase the chances of reaching its target audience, but would also increase ad engagement, click-through rates and conversions.

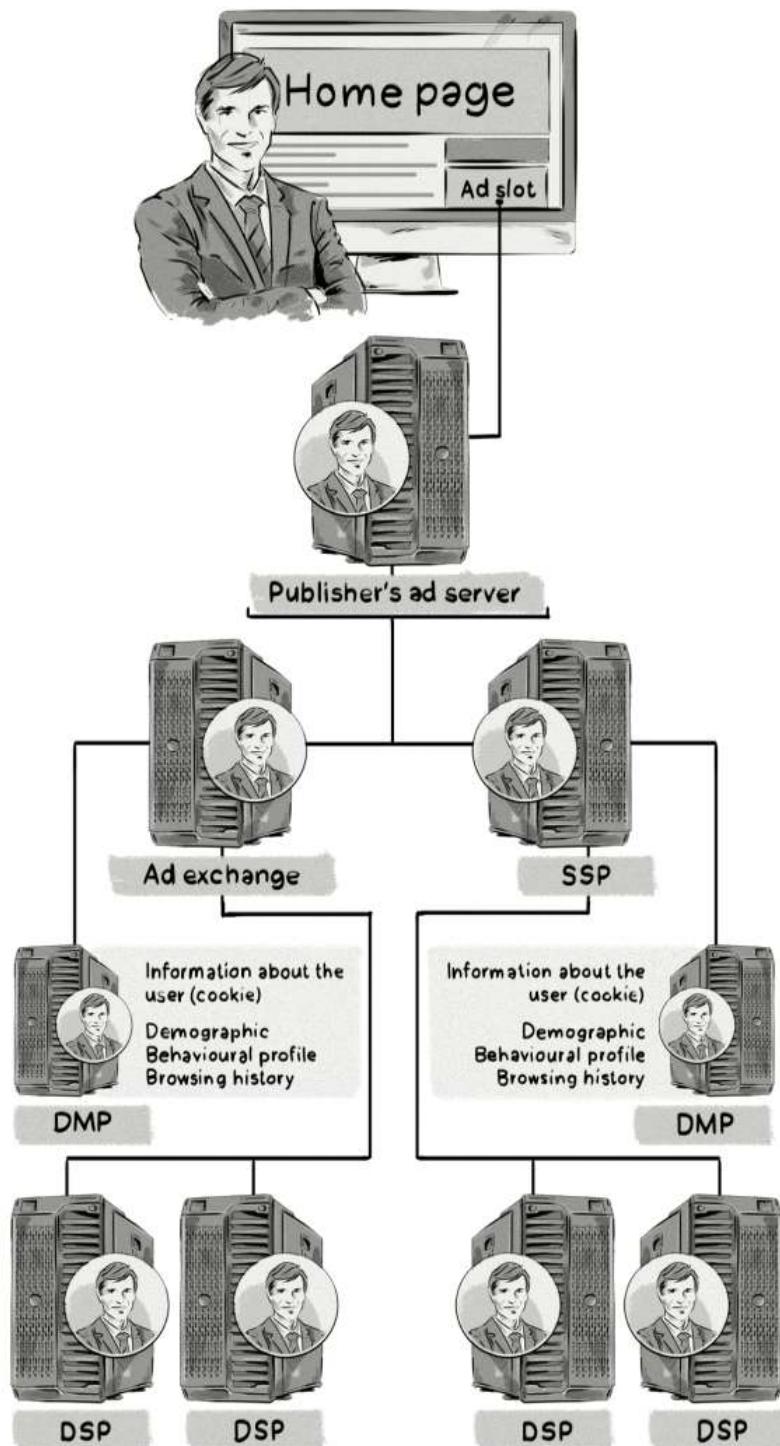
Behavioral Targeting

Behavioral targeting, also known as online behavioral advertising (OBA), allows advertisers and publishers to display relevant ads and marketing messages to users based on their web-browsing behavior.

The types of data collected for behavioral targeting include:

- Pages viewed
- Previous search terms
- Amount of time spent on a website
- Ads and buttons clicked
- Content viewed and downloaded
- Purchases
- Date of the last website visit
- Other information about their interactions with various websites

Online behavioral targeting



Online behavioral targeting uses information about the user to determine which ads to display.

The behavioral targeting process consists of three main steps:

1. Data Collection

Advertisers, publishers, and DMPs collect data about the actions users carry out across different websites. This data is often referred to as event data and includes page views, products views, products purchased, and other interactions on a website or mobile app. This data is then tied together via identifiers stored inside third-party and first-party cookies in web browsers, or mobile IDs in mobile apps.

User profiles are then created to store a given user's event data in one place and assign all future event data to that user profile. An identifier, such as an ID in a third-party cookie or a mobile ID, would be used to link a user with their actions across different websites and assign the event data to the right user profile.

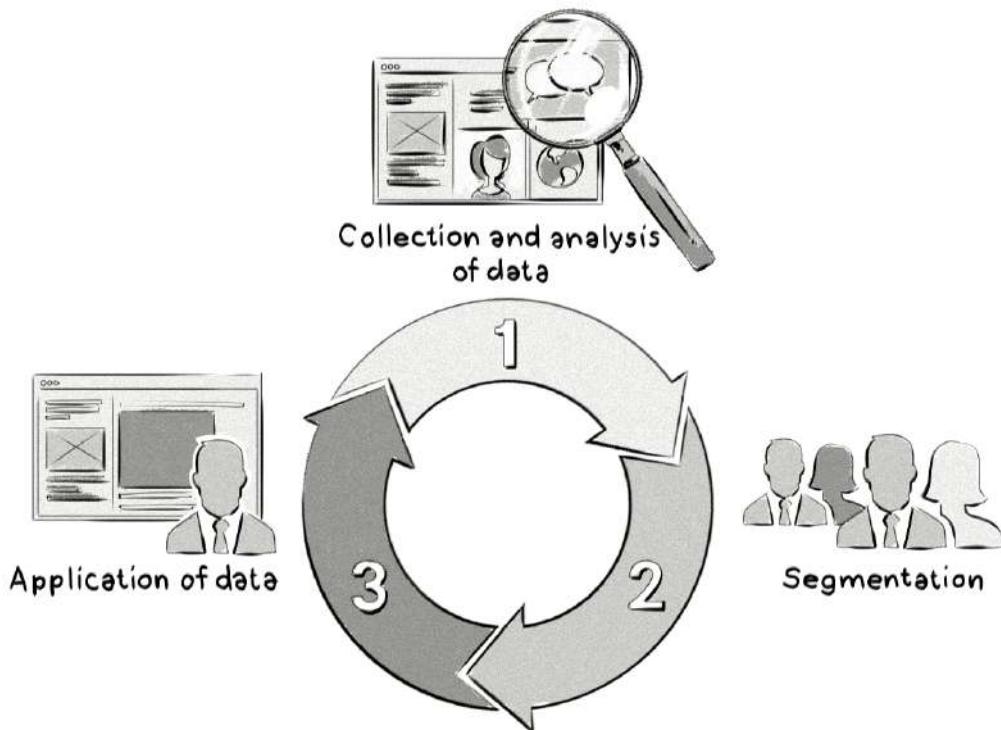
2. Audience Creation

Advertisers and publishers then create audiences that are made up of individual user profiles.

For example, an advertiser could create an audience that includes people who have viewed a given product more than three times in a month, signed up for a newsletter, and have visited their website at least 15 times in the past 60 days.

3. Application of Data

The advertiser then uses those audiences for ad targeting in its online media campaigns, resulting in the ads being more relevant to the users and increasing the chances of them converting (e.g. purchasing a product).



The three main steps of the behavioral targeting process.

Benefits of Behavioral Targeting

The amount of data marketers have about users allows them to create very detailed profiles and display ads relevant to each audience accordingly.

The premise behind behavioral targeting is that it benefits the visitor as much as it benefits the website displaying the ads – i.e users are shown ads that they are actually interested in, which improves the user experience of the website.

However, online users have become aware of how online advertising companies collect and use their data, which has resulted in some users becoming concerned about this type of targeting and resulted in the rise of ad-blocking software.

Challenges of Behavioral Targeting and the Impact of the GDPR

With privacy laws like the [General Data-Protection Regulation \(GDPR\)](#) in effect, this targeting method became challenged by stricter rules concerning storing cookies in a user's browser.

The EU law forced marketers to reduce their dependence on behavioral data and look for new targeting methods that don't rely heavily on collecting and using personal data.

In addition to privacy laws, there are also privacy settings in popular web browsers, such as [Safari's Intelligent Tracking Prevention \(ITP\)](#) and [Firefox's Enhanced Tracking Protection \(ETP\)](#), that block third-party cookies by default and put restrictions on other types of cookies. Google Chrome, which is the most popular web browser globally, will also turn off support for third-party cookies in 2022.

In addition to the privacy changes in web browsers, Apple has made some changes to how its identifier for advertisers (IDFA) can be accessed by app developers and AdTech companies to increase user privacy.

These privacy changes make running behavioral advertising campaigns extremely limited, if not impossible.

In a privacy-first world, some advertising platforms that previously prided themselves on their behavioral-targeting capabilities are now turning to contextual advertising, where the power lies in minimized reliance on personal data.

However, due to the huge time, cost and resource investments AdTech and data-collection companies have made in collecting and using behavioral data, this shift is a slow one.

Please refer to chapter 14. User Privacy in Digital Advertising for more information about these privacy topics.

Retargeting

Retargeting involves showing ads to online visitors who have interacted with the brand in the past.

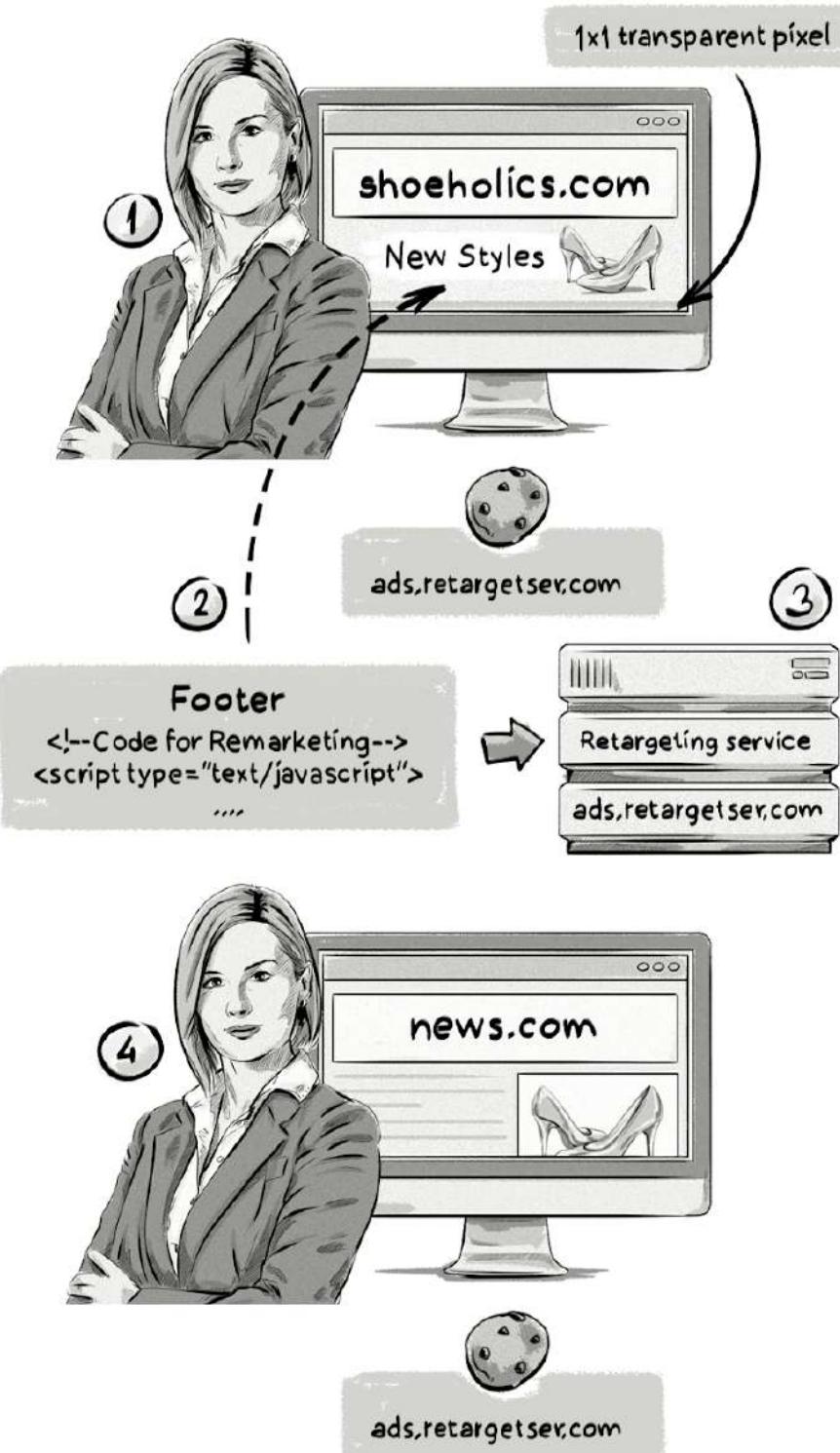
For example, if an online visitor views a pair of shoes, then they'll likely see the same pair of shoes (or even different ones) advertised on different websites.

The process works by placing a 1×1 transparent image (a pixel) on a website. Then, when the page loads, the pixel sends a request to an AdTech platform (e.g. a demand-side platform) to retrieve the 1×1 transparent image.

As the image is returned to the web browser, the DSP creates a cookie, if one wasn't created previously, and saves it on the visitor's device.

Then, when the visitor accesses a different website, the DSP is able to identify that user and show them the retargeted ad – i.e. the shoes they viewed on the previous website.

Here's a visual representation of how retargeting works:



Here's an overview of what's happening in the image above:

1. An online shopper visits shoeholics.com and views a pair of shoes.
2. The retargeting service's code located in between the <footer> tags sends a request for a 1×1 pixel.
3. The retargeting service sends back the 1×1 pixel and saves a cookie to the shopper under their domain (ads.retargetser.com), storing information about the shopper and their behavior, such as the product they viewed.
4. The shopper leaves shoeholics.com and visits a different website — news.com — and sees an ad for the exact same pair of shoes that they were looking at previously.

The DSP is able to identify the same visitors across different websites by syncing cookies with other AdTech platforms – for example, supply-side platforms (SSPs) and ad exchanges.

Similarly to behavioral targeting, many online visitors have come to dislike retargeted ads, as they appear to "follow" visitors around the internet.

*Please refer to the **11. Data Management Platforms (DMPs) & Data Usage** chapter for more information about cookie syncing.*

Demographic

Demographic targeting is one of the most powerful forms of targeting and can be used in combination with other methods to really refine the targeting criteria. At the same time, it's very tricky because most publishers don't ask nor collect this type of information from their visitors, except for companies like Facebook and Google.

Examples of demographic information include, but are not limited to:

- Age
- Gender
- Annual income
- Marital status
- Parental status
- Occupation

So, for example, if an advertiser wanted to display ads promoting baby products to female users, between 20 and 40 years of age, who have one child or more, it could use demographic targeting and other targeting methods to display ads to the right visitors.

With campaigns run on independent AdTech platforms (i.e. not via Google, Facebook, LinkedIn, etc.), advertisers can use demographic targeting by using audience segments in their DMP or via the data contained in the *User* object in OpenRTB bid requests.

When running campaigns using demographic data on Google and Facebook and other platforms that collect this type of data directly from users, advertisers simply need to set up the targeting criteria inside those platforms.

An example of how to use demographic targeting when advertising on Facebook.

Controlling a Campaign's Budget

When running an ad campaign, advertisers not only focus on making changes to **improve** its effectiveness by adjusting the message, placement, targeting, etc., but also aim to **reduce** ad waste by optimizing and improving the efficiency of their campaign's budgets.

What is ad waste?

Ad waste is inventory that the advertiser paid for but didn't reach the target audience – e.g. was shown to the wrong audience or a bot.

There are a number of factors that can cause an ad to be deemed wasted, including viewability, ad fraud, incorrect frequency. We cover these areas throughout the book.

Below are just a few areas advertisers look at when controlling and managing their campaign budgets, all of which can be implemented in an ad server or DSP:

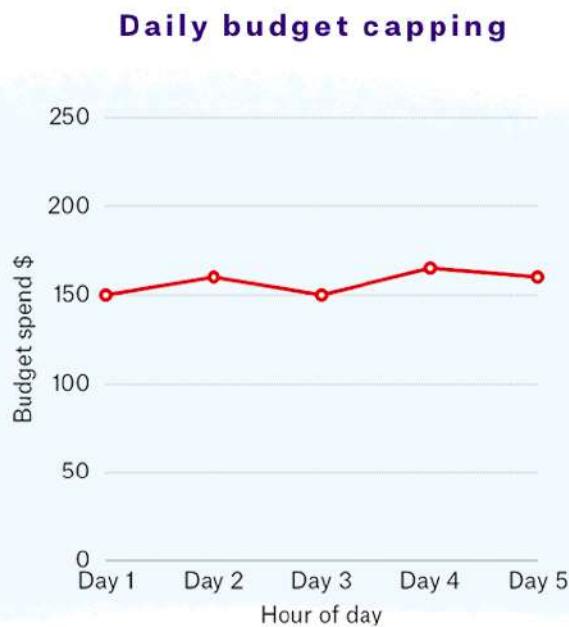
Budget Capping

Adding a budget cap to an ad campaign sets a limit on how much money will be spent.

For example, you could set a daily budget cap of \$150, meaning that once the campaign has spent that amount of money, no more ads will be shown that day.

Limiting a campaign's budget involves putting a total and daily cap on the amount of money a campaign spends. In this case, once the daily budget has been spent, the campaign will stop for that day.

Some platforms will add a certain percentage (e.g. 20%) on top of the daily budget to help advertisers get the most out of their campaign



The image above illustrates how a maximum daily budget could be spent.

The daily cap can be larger to make up for the under-delivery of ads on certain days, but it may cause the campaign to stop prematurely.

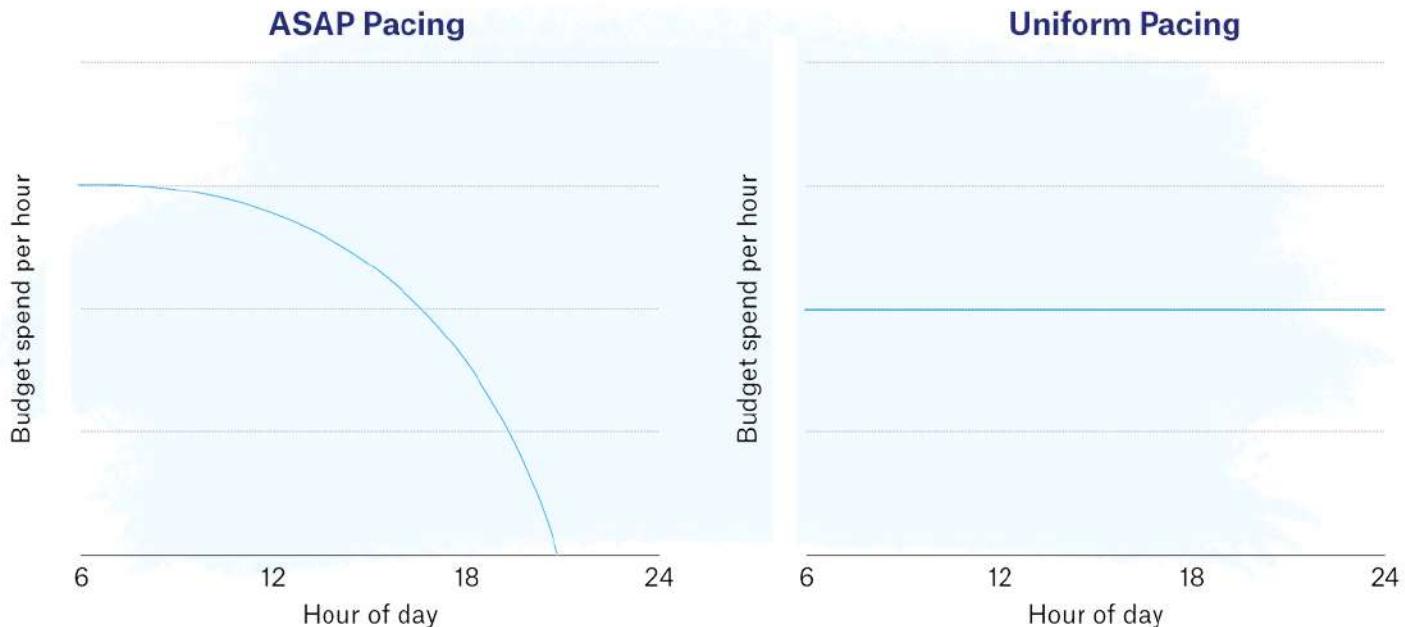
Budget Distribution (aka Pacing)

Pacing refers to how quickly or slowly the budget of the campaign is spent, which impacts how many impressions are served to online consumers over any given period during the campaign's lifetime.

For example, you may want to get your ads in front of as many consumers as quickly as you can, so you would choose to deliver the maximum number of impressions as soon as possible, known as **ASAP pacing**.

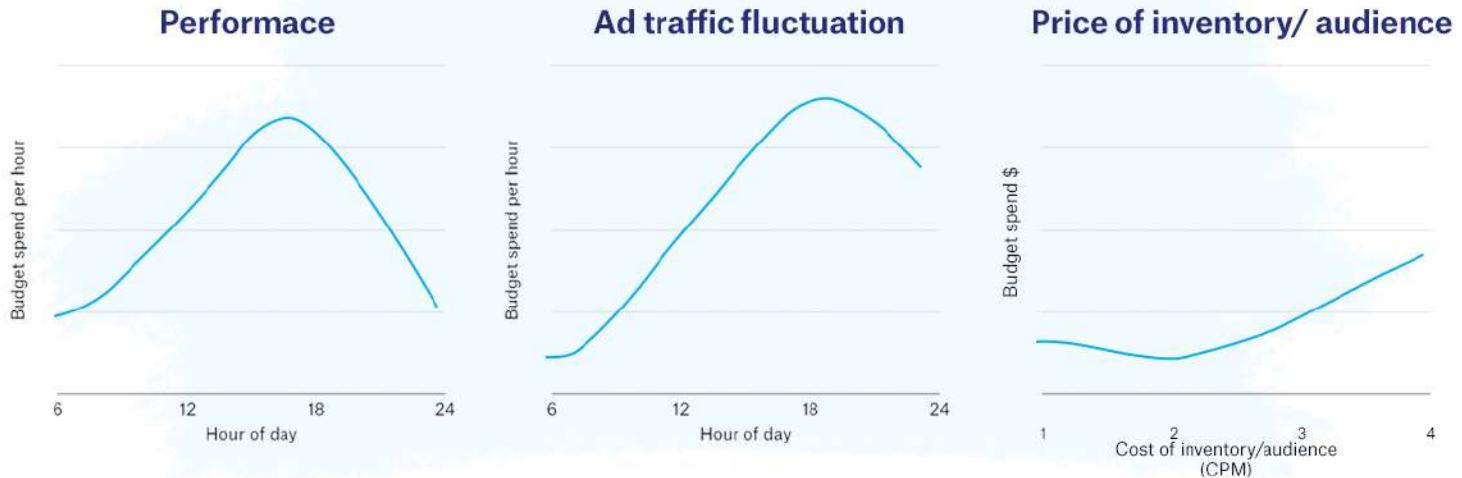
Alternatively, you may choose to distribute your ads evenly and allow them to run for the duration of the campaign's proposed dates, known as **uniform pacing**.

Examples of ASAP and uniform pacing:



In the real world, pacing also has to account for the fluctuation of ad traffic throughout the day and the availability of the ad impressions matching the campaign's targeting criteria.

Ad platforms can adjust the speed in which they spend the campaign budget based on performance, availability of traffic, and price of the inventory/audience:



Frequency Capping

Frequency capping involves limiting the number of times the same ad is shown to a given visitor.

For example: three impressions per visitor per 24 hours.

Frequency capping is important because it:

- Limits budget waste.
- Helps to improve a campaign's overall reach.
- Prevents so-called “overexposure” (a user's frustration over seeing the ad multiple times).

Google Ads | New campaign

1 Create your campaign 2 Confirmation

Frequency capping Limit how many times that ads in this campaign can show to the same user [?](#)

Cap impression frequency [?](#)
Limit how many times that ads in this campaign can show to the same user

Impressions cap	Frequency
10	per day

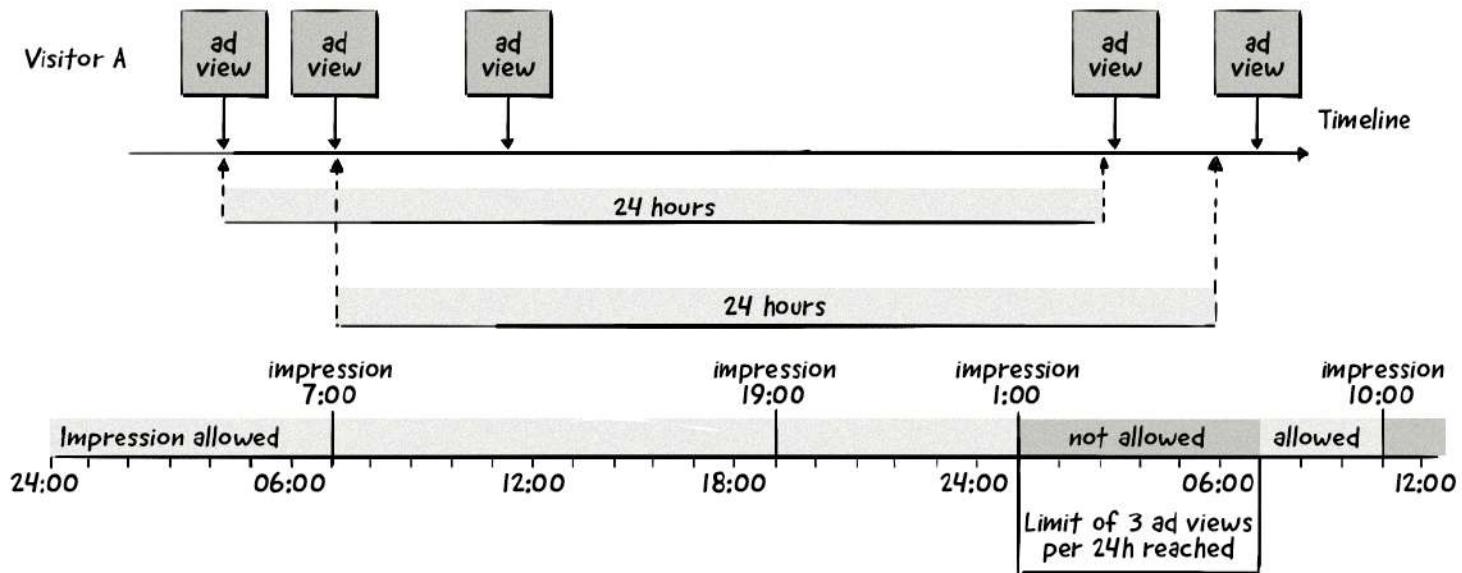
[ADD IMPRESSION CAP](#)

Cap view frequency [?](#)
Limit how many times that ads in this campaign can get a view or interaction from the same user

An example of implementing frequency capping in Google Ads.

Let's see a frequency-capping example:

Three impressions per visitor per 24 hours



Each time frequency capping is evaluated, the number of impressions within the period of time is counted.

For a 24-hour cap of three impressions, the impressions could fire at 7:00, 19:00, 1:00 the next day and 10:00 the next day. The user will never see the same ad more than three times within a 24-hour period.

How Is Frequency Capping Implemented?

First, the ad server registers and stores the number of times an ad (impression) from a particular campaign is displayed to a consumer based on their identifiers (e.g. cookies, device IDs, device fingerprints, etc.).

Then, it stores this information server-side (i.e. in the ad server) along with the user's identifier.

This information is often referred to as ***user profiles*** on AdTech platforms.

Every user profile contains the information associated with the given cookie ID or device ID, such as the ads that the user was exposed to.

They are typically stored in in-memory or other fast-access databases so that the information can be quickly fetched during the decisioning process of the ad server.

Why not store this information client-side (i.e. in a third-party cookie)? Here are a couple of reasons:

- The cookie size would dramatically increase. Instead of storing a single ID, we would have to store each ad ID with the corresponding impressions and their time.
- It's not portable to other visitor-identification technologies, such as device IDs (AdID / IDFA).

Chapter Summary

- There are many different targeting methods that advertisers can use.
- The most popular ones are contextual, behavioral, and demographic.
- Advertisers can control their advertising budgets by setting daily and campaign caps, as well as using pacing and frequency capping.

08. Tracking and Reporting Impressions, Clicks, and Conversions in AdTech Platforms



In the previous chapters of this book, we looked at how advertisers and publishers use AdTech platforms to set up and run campaigns.

In this chapter we'll take a look at how AdTech platforms collect data so advertisers and publishers can track and view detailed reports about the performance of their campaigns.

Most of the explanations and examples in this chapter illustrate how tracking and reporting works in both a publisher's and an advertiser's ad server, but many other platforms like DSPs and SSPs also include these functionalities.

Impression, Click, and Conversion Tracking

Tracking is an important part of an AdTech platform and is the first step in understanding the performance of an ad campaign and measuring key metrics.

Essentially, tracking involves gathering data about an ad campaign.

There are a number of areas that AdTech platforms track, including basic metrics like impressions, clicks and conversions, and others like viewability and ad-exposure time. They can also track metrics from video ads, such as plays, completion rates, and average time played.

Impression Tracking

Impression tracking is quite simply tracking the number of impressions each ad receives.

An impression is counted each time it is displayed to a user.

For example, if a user visits a web page and sees an ad, then reloads the page and sees the exact same ad again, two impressions would be counted.

The most popular method of counting an impression is to serve a 1×1 transparent image that notifies the ad server of an impression. It's called an **impression tracker** (or **impression pixel**).

The ad server returns a pixel in the ad markup to count the impression when the browser renders the ad markup – as opposed to counting it when the ad server selects the ad – and returns the ad markup to the browser.

This way, the ad impression is counted when the browser loads the creative.

Here's an example of an impression tracker from the Google Ad Manager ad server (formerly DoubleClick For Publishers):

```
<IMG SRC="https://ad.doubleclick.net/ddm/trackimp/Nxxxx.site-
keyname/Byyyyyyy.n;dc_trk_aid={ad_id};dc_trk_cid=
{creative_id};ord=
[timestamp];dc_lat=N;dc_rdid=Czzzz;tag_for_child_directed_treatm
ent=I?" BORDER="0" HEIGHT="1" WIDTH="1" ALT="Advertisement">
```

The ad server can include a number of additional pixels in the ad markup from third-party AdTech platforms in order to count the impression in multiple systems – e.g. a third-party ad server used only for measurement or an ad-verification platform.

This process of loading other tags or pixels making calls to other platforms is known as **piggybacking**.

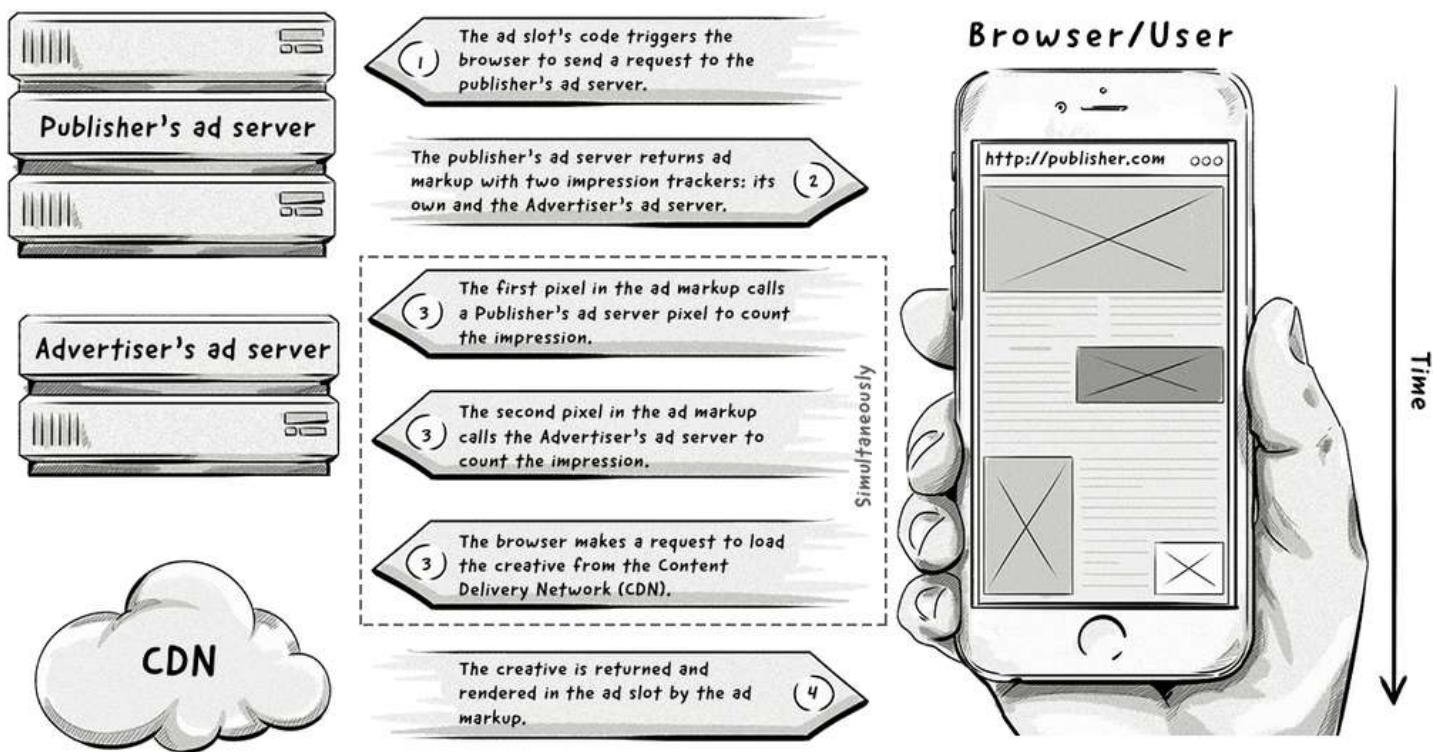
There are two main methods of counting an impression in both the publisher's and advertiser's ad servers:

Method 1

The publisher's ad server includes two 1×1 pixels in the ad markup.

The first pixel sends a **request to the publisher's ad server**, which counts the impression, and the second pixel sends a **request to the advertiser's ad server**, which also counts the impression.

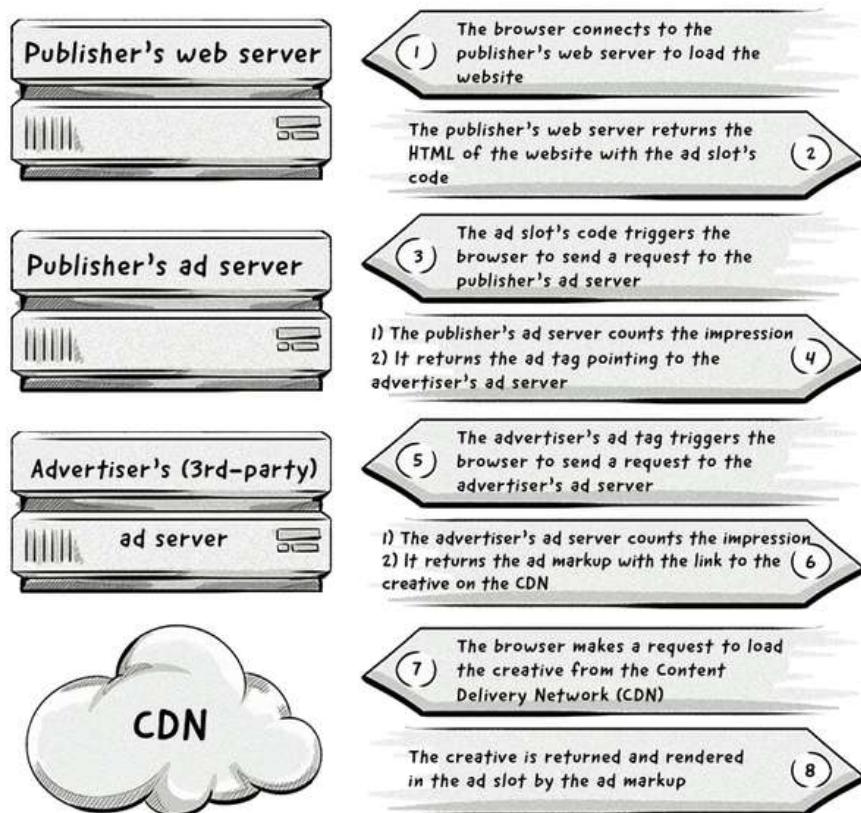
Both pixels are sent to their respective ad servers at the same time.



Impression tracking: Method 1

Method 2

Both the publisher's and the advertiser's ad servers count the impression **only when their respective ad servers have received a request for an ad**.



Impression tracking: Method 2

Click Tracking

Tracking the number of clicks an ad receives is typically done via a **click tracker**.

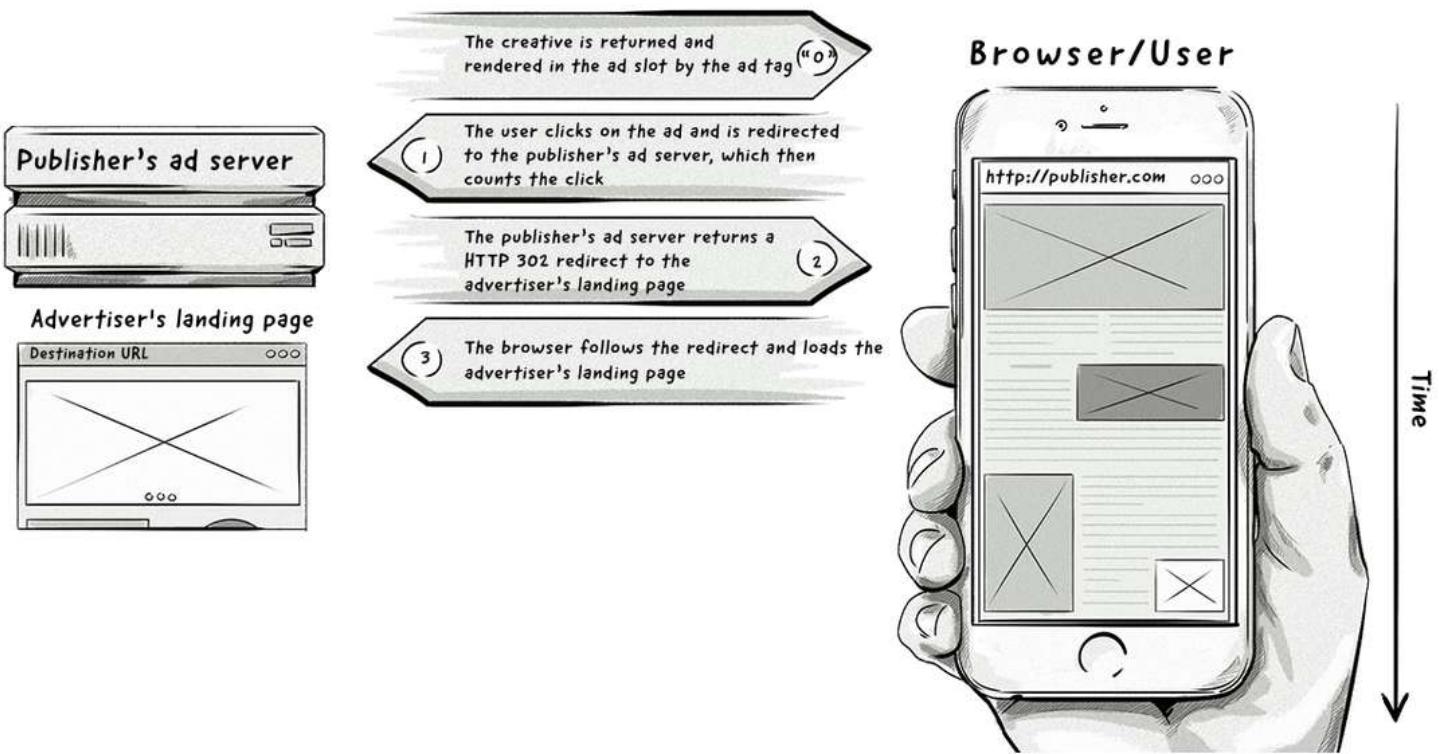
A click tracker is the URL of the ad server's redirect service, which counts the click and redirects the visitor to the final landing page of the campaign.

The ad server returns the click tracker in the ad markup in order to count the click before the visitor is redirected to the final landing page.

Below is an example of a click tracker from the Google Ad Manager ad server:

```
http://pubads.g.doubleclick.net/gampad/clk?
id=123456789&iu=/1234/adunit&t=page%3Dsports
```

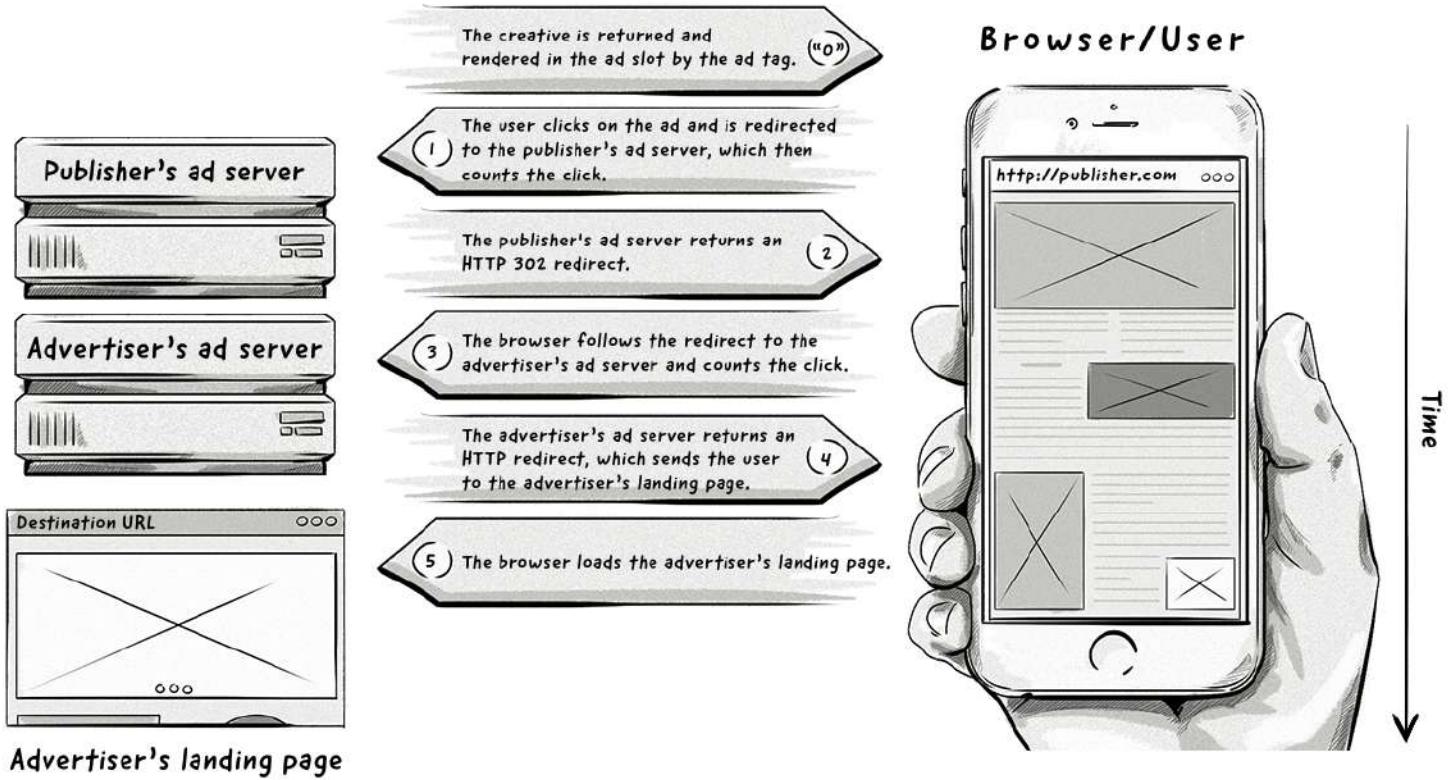
Here's the basic flow of how a click tracker works:



How click tracking works in a publisher's ad server.

The diagram above illustrates how click tracking works with a publisher's ad server, but what if the advertiser wants to track the click as well?

To achieve this, they would need to add a click redirect from the publisher's ad server to the advertiser's ad server, then redirect the user to the landing page.



How click tracking works in a publisher's and advertiser's ad servers.

The reason why the advertiser's ad server would also count the same click and impression is to verify the reports provided by the publisher by comparing the number of impressions and clicks, as well as to aggregate all campaign data in one system (i.e. the advertiser's ad server).

It is possible to add a lot more redirects to conduct more processes, such as:

- Ad verification to detect viewable impressions, bots, and fraudulent activity.
- Tracking clicks in middlemen systems, such as ad networks.

Click URL Macros

Click trackers can support passing the destination URL as a parameter (e.g. `redir_url=`). This functionality is necessary to add multiple click trackers in the redirect chain and pass the URL of the next redirect dynamically to the click tracker.

Typically, when we paste a click tracker in the ad server, we can use the **click URL macro** to expand the URL of the next click tracker in the chain.

Here's an example:

```
https://ad.example.org/click?ad_id=123456&redir_url=%click_url%
```

The ad server automatically expands the `%%CLICK_URL%%` placeholder to the next click tracker in the chain (i.e. its own click tracker). For example:

https://ad.example.org/click?ad_id=123456&redir_url=http://ad.doubleclick.net/clk%3B246885467%3B71938114%3Bx%3B

Conversion Tracking

A **conversion** is registered every time a user completes a goal set by an advertiser or marketer.

A goal could be to get consumers to purchase a product, download a file, or even fill in a contact form on a landing page. Each time a consumer completes one of these actions, a conversion will be recorded.

In online advertising and marketing, conversion tracking is used to report on campaign performance. Also, it is used in conjunction with the cost-per-action (CPA) model where publishers and affiliate advertisers/marketers only receive payment once a conversion is registered.

There are two main types of conversions: **click-through conversion** and **view-through conversion**.

Click-through is when a user has clicked on an ad AND converted.

To calculate the click-through conversion (CTC) rate, you divide the number of conversions by the number of clicks that ad received.

$$\text{CTC \%} = (\text{conversions} \div \text{clicks}) \times 100$$

View-through is when a user has seen an ad AND didn't click it BUT converted.

For example, if they saw an ad for a pair of shoes, but instead of clicking on the ad and purchasing them, they went to the website directly and purchased them.

To calculate the view-through conversion (VTC) rate, you divide the number of conversions by the number of impressions the ad received.

$$\text{VTC \%} = (\text{conversions} \div \text{impressions}) \times 100$$

The CTC and VTC rates will vary widely from one advertiser to another, as there are a number of factors at play, such as the product or service the advertiser is promoting and the audience exposed to the ads.

What is an attribution window?

With both conversion models, there is something called an **attribution window**, which refers to the time between when a user first saw or clicked on the ad and the time they actually converted.

The attribution window varies between advertisers, but it can be anywhere from 24 hours to 30 days.

Finding the right attribution-window time frame can be tricky because the longer an attribution window is, the less accurate the attribution becomes.

It can be difficult to know whether a user converted because they saw an ad 30 days before the conversion or because they were persuaded to convert via some other advertising channel.

Similarly, if the attribution window is too short, it could exclude some users who were exposed to the ad and converted as a result of seeing the ad. This not only affects the advertiser's attribution reports, but also impacts the publisher's potential revenue.

The advantages and disadvantages of these two types of conversions are as follows:

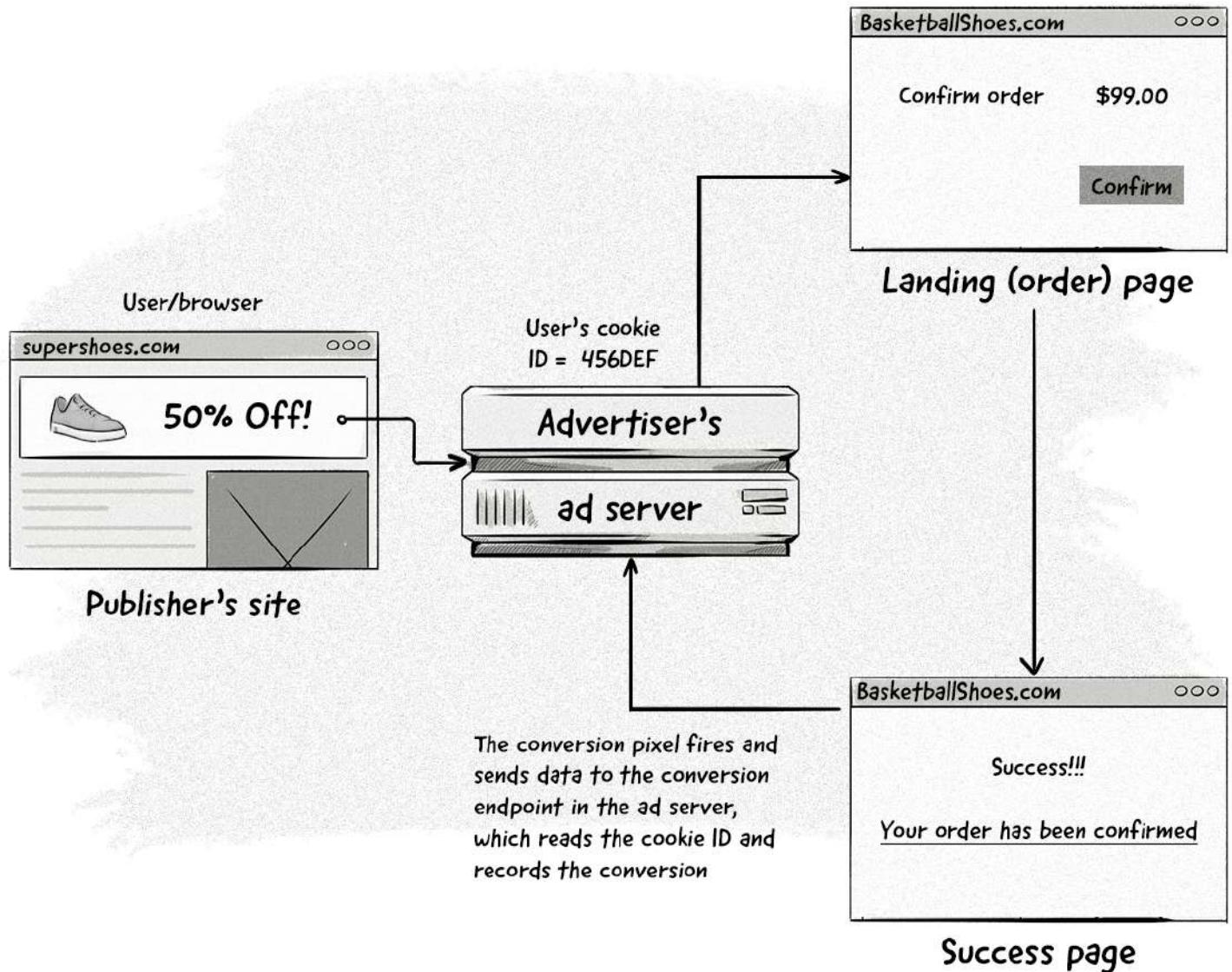
	Click-through conversion	View-through conversion
Advantages	Allows advertisers to accurately attribute the clicks to conversions, leaving little or no room for inaccurate reporting.	Depending on the product or service being promoted, this type of conversion can work better for middle- and top-funnel campaigns than for click-through conversions.
Disadvantages	One of the main disadvantages of this method has more to do with the attribution model than the click-through conversion itself. For example, if you use the first or last click-attribution model, it can be hard to know if that click was the event that actually influenced the user to convert.	It's possible that the ad was displayed to the user, but they may not have actually seen it (the ad might not have been in the viewport of the browser) or been influenced by it. In other words, it's possible to attribute too many conversions to the campaign. Conversion attribution may be lost if a visitor deletes their cookies in the time between seeing the ad and converting. This method is also more prone to fraud. For example, it's possible that the pixel could be fired without the actual creative being shown. Then, if the user converts, it will be recorded as a view-through conversion, despite the user never actually seeing the ad.

These two types of conversions are part of a larger and broader field of online advertising and marketing known as attribution, which takes into account a number of different interactions a visitor has with a brand or ad.

Apart from there being different types of conversions, there are also different conversion-tracking methods:

The Pixel Method

The pixel method for **click-through tracking** works like this:

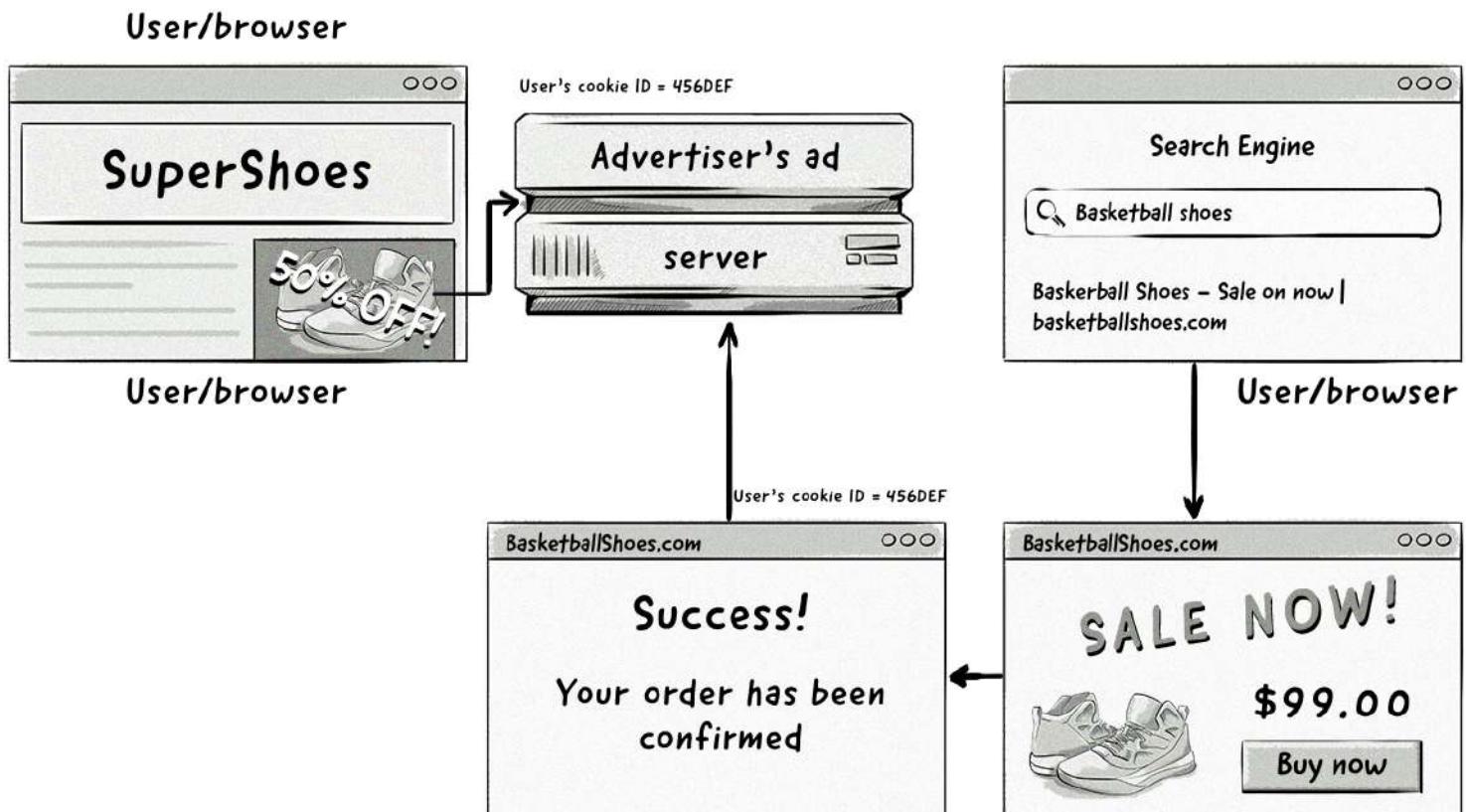


In the pixel method for click-through conversions, the user visits a website, sees an ad and clicks on it. They are then taken to the advertiser's landing page and convert. When the user clicks on the ad, the advertiser's conversion pixel fires and records the user's cookie ID in the advertiser's ad server.

Typically, an ad server will assume that the last click ID for the particular cookie ID generated the conversion.

This way, the conversion can be associated with a specific ad, line item, and campaign (the click ID will store information about which ad the user clicked).

The pixel method for **view-through tracking**:



In the pixel method for view-through conversions, the user sees an ad (but doesn't click on it), leaves the publisher's website, comes back to the advertiser's website through another channel (e.g. via a Google search), and then converts.

The advertiser is able to attribute the conversion to the ad that was on the publisher's website by comparing the cookie ID it created when it displayed the ad on the publisher's site with the one created when the conversion pixel fired on the success page.

The Server-Side Method

The server-side method works in a similar way to the pixel method; however, instead of firing a pixel and passing the user's cookie ID to the ad server, the user's cookie ID is passed from the page to the ad server via a server-to-server call.

This method is widely used in the affiliate advertising and marketing space because it is so crucial to get the data right and reliably track the conversions for the partners (i.e. publishers) because they get paid only for conversions.

Below are a couple examples to help explain the server-side method:

Example 1: Selling insurance as an affiliate

Affiliate advertisers and marketers are paid on a cost-per-action/acquisition (CPA) basis, which means they only receive payment, either in the form of a fixed-priced commission or a percentage of the sale's total value, when a user converts.

However, it could be hours, days or even weeks between the time a user sees the insurance ad on the publisher's site and the time they actually convert (purchase the insurance policy).

Therefore, the system on the advertiser's side must track the click ID and notify the affiliate ad network (or the ad server) about the successful conversion once the conversion is verified – e.g. when the application is processed successfully or when payment from the user is received.

Example 2: App installs

Attributing a conversion for an app install to a publisher or affiliate advertiser/marketer is different than attributing conversions in browsers. The reason for this is because, unlike web and mobile browsers that are able to fire pixels, there is no way to fire a pixel in a mobile app.

In order to track events such as conversions, the software-development kit (SDK) in the app has to notify the ad server of the installation, which is then attributed to the app-store redirect generated by the partner (i.e. publisher or affiliate).

A postback notification is sent to notify the publisher or affiliate about the successful install, meaning they have just earned a CPA commission.

The Importance of Properly Attributing Affiliate Campaigns

As you can probably imagine, trust is an issue that often arises with CPA campaigns.

There are a few ways advertisers can evade paying commissions to publishers and affiliates, but this ultimately disadvantages the advertiser as well as the publisher or affiliate.

Let us explain.

In the affiliate, CPA, and revenue-sharing space, publishers can ultimately choose from hundreds of offers to promote.

The publisher's and affiliate's goal is to make the most money possible from the offers they promote, so most of them will test the offers on a small percentage of their traffic and tweak them to find the ones that generate the most revenue.

If the offers don't perform well, which could be due to a number of reasons (such as offers not being the right fit for their audience), they will simply remove them from their site and stop promoting them, which means the advertiser won't receive any conversions from the offers.

This essentially defeats the point of the whole process.

Reporting

The reporting function of an AdTech platform is responsible for displaying metrics about many different areas of a campaign.

The reports are highly valuable for both advertisers and publishers, as they provide clear insights into the performance of their campaigns and the users who click on their ads.

For every impression served, an AdTech platform stores a record with the following attributes:

- Timestamp (impression, click, conversion)
- IP address
- Campaign ID
- Line item ID
- Ad/creative ID
- Geolocation
- Browser
- OS
- Publisher domain
- Publisher placement
- ... and others

Similar information is stored for every click and conversion.

Dimension

Filters

Country	Impressions	Clicks	CTR	Conversions	...
Poland	1,000,000	100	0.01%	7	...
Germany	1,000,000	150	0.015%	5	...
UK	1,000,000	75	0.0075%	10	...
...

Metrics

Metrics

A **metric** is an actual number calculated for the overall campaign or the data matching the specific dimension's value.

Some metrics can be derived from others; for example, calculating the CTR metric is done by dividing the total number of clicks (metric) by the total number of impressions (metric):

$$CTR = \text{clicks} / \text{impressions} \times 100.$$

Examples of metrics include:

- **Impressions:** the number of times an ad was displayed.
- **Clicks:** The number of times an ad was clicked on.
- **Conversions:** the number of desired actions (goals) performed by a user (e.g. filling in a contact form or making a purchase).
- **Reach:** the number of unique visitors/devices that the campaign reached.
- **Click-through rate (CTR):** number of clicks / number of impressions $\times 100$.
- **Cost per mille (CPM):** cost per 1,000 impressions.
- **Cost per click (CPC):** the cost of each click an ad or link generates.
- **Cost per action/acquisition (CPA):** the cost of each action, acquisition, or conversion. CPA is often used in affiliate marketing.
- **Conversion rate (CVR):** the number of conversions divided by the number of clicks (then multiplied by 100 to get a percentage). This model is typically used for click-through conversions.

- **Amount spent (cost):** the amount of money spent for the respective impressions, clicks and conversions.
- **Revenue (total conversion value):** the amount of money earned from the conversions.

Effective Cost Per Mille, Click, and Action (eCPM, eCPC, eCPA)

In most reports, you'll see metrics that have the letter **e** before them.

The **e** stands for **effective** and is used to determine the revenue generated by a particular pricing model (e.g. eCPM).

Effective CPM, CPC, and CPA can be calculated for any campaign and can be worked out by using the following formulas:

Effective cost per click (eCPC) = budget spend / number of clicks

Effective cost per action/acquisition (eCPA) = budget spend / number of conversions

Effective cost per mille (eCPM) = budget spend / number of impressions x 1000

As advertisers and publishers select a pricing model before the campaign starts, these pricing models show advertisers and publishers what the results would have been if they had used that particular pricing model.

Very often, advertisers will calculate their campaigns in different pricing models to compare their performance.

On the publisher's side, they may want to calculate the eCPC or eCPA for all their CPM campaigns to see if they could have made more revenue via those pricing models.

For example, let's have a look at the following three campaigns:

Campaign #1: CPM

Campaign	Impressions	Clicks	Conversions	Total cost	CPM	eCPC	eCPA
Summer promotion	1,000,000	1,500	10	\$4,000	\$4	\$2.67	\$400

Campaign #2: CPC

Campaign	Impressions	Clicks	Conversions	Total cost	eCPM	CPC	eCPA
Summer promotion 2	1,000,000	2,000	50	\$10,000	\$10	\$5	\$200

Campaign #3: CPA

Campaign	Impressions	Clicks	Conversions	Total cost	eCPM	cCPC	CPA
Summer promotion 3	1,000,000	2,500	80	\$15,000	\$15	\$6	\$187.50

The table above shows the eCPM, cCPC and CPA for the three campaigns.

In performance-based advertising, advertisers will look at the return on investment (ROI) of the campaign and traffic source. This metric is used to evaluate the efficiency of their advertising budget.

It is calculated in the following way:

$$\text{ROI} = (\text{total conversion value} - \text{amount spent}) / \text{amount spent} \times 100\%$$

The ROI metric will have positive values when the advertiser is making money and negative values when the advertiser is losing money.

Example:

	Total conversion value	Amount spent	ROI	
Campaign 1	\$1,200	\$1,000	+20%	For every dollar spent, we earn 20 cents*
Campaign 2	\$900	\$1,000	-10%	For every dollar spent, we lose 10 cents*

*This does not take into account any fixed or variable costs that you may have with delivering goods or services to the end customers, so even a 20% ROI may not necessarily mean that you make profit – however, this works very well with digital goods where your marginal cost is very low.

Dimension and Subdimensions

A **dimension** is an attribute or variable of data used to break down a report.

Some examples of dimensions include:

- Country
- Device type
- Browser type
- Hour of the day
- Campaign
- Line item
- Creative

- Date, day of the week
- Publisher URL/domain
- OS and OS version
- Geolocation

Subdimensions (aka **drill-downs**) allow us to view data from a given dimension that's broken down by another dimension (e.g. Country -> Carrier -> Line item -> Ad).

Filtering

Filtering (aka **segmentation**) allows you to restrict the data set that you are running the report on.

Common filters include:

- Date range
- Advertiser -> Insertion Order -> Line Item -> Ad

On top of that, you can typically apply an include/exclude filter for any value for any dimension, e.g.:

- Country = Poland OR Germany OR United Kingdom
- Device type = Tablet
- Day of week = Monday-Friday

Technical Considerations of Reporting

From an ad-operations perspective, there are some important aspects of reporting that need to be acknowledged, otherwise the advertiser or publisher could be confused and misled when comparing data from other systems.

Delays

There is usually a delay between the time an event is received by the system and the time it's included in the reports. Most of the time, it is a few minutes, but sometimes, it can be as high as a couple of hours.

The most recent data is often an approximation of a complete report, and an accurate report is available after some time. It's best to check these values for the reporting system that you are using.

An example of a data delay:

Report-data approximation is available within 15 minutes of an event occurrence, with an accurate report available within a maximum of 24 hours. Typically, the accurate report should be used for billing purposes.

Reporting Time Zone

When comparing reports from different systems, it is important to determine whether they are both using the same time zone and that only accurate data is used (not an approximation).

Data Retention

Some reporting systems handle the increase in data by dropping events older than some threshold age (e.g. six months or one year). An alternative space and cost-saving technique is to decrease report granularity with

time.

For example, data from the last month is available with precision up to an hour, data from one month to one year is summed up for the entire day, and data older than one year is only available in the form of campaign totals.

Discrepancies: Trust, But Verify

In online advertising, a discrepancy is the difference between reported data in two different AdTech platforms – e.g. between a publisher's ad server and an advertiser's ad server.

It is a very sensitive topic because the data collected by these AdTech platforms is later used for billing purposes and is often subject of disputes between publishers, advertisers, and AdTech vendors.

While there can be a number of reasons for discrepancies, most can be attributed to technical errors.

A majority of AdTech platforms depend on client-side tracking methods – i.e. those carried out in web browsers, SDKs in mobile apps, and other embedded devices – for receiving data about events, such as impressions, clicks, and conversions.

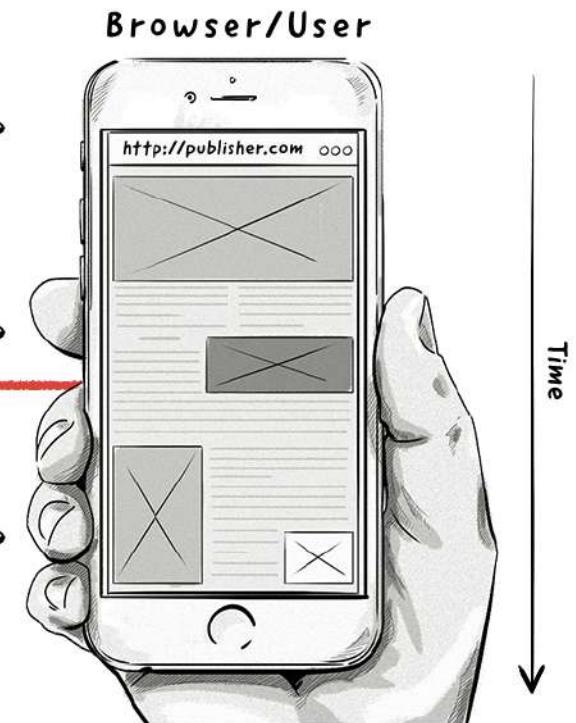
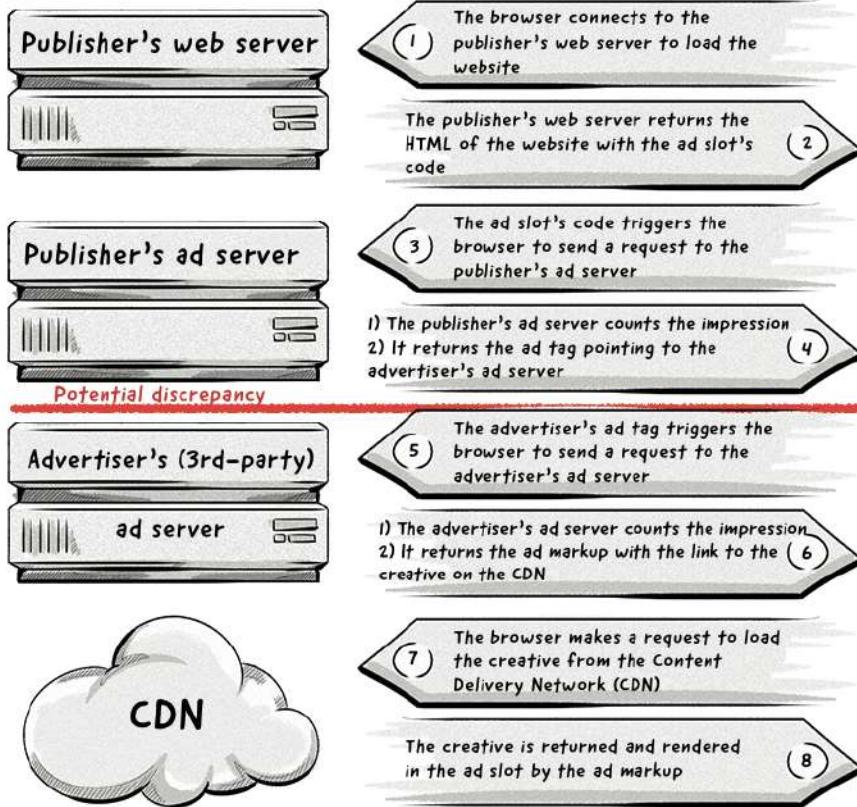
The issue with client-side tracking is that it is error prone (*more on the causes below*).

In this section, we'll answer the following questions:

- How can one verify whether a publisher's ad server or an advertiser's ad server reports are valid?
- Why are discrepancies inevitable?
- What are the common causes of discrepancies?
- What is the acceptable level of discrepancies?

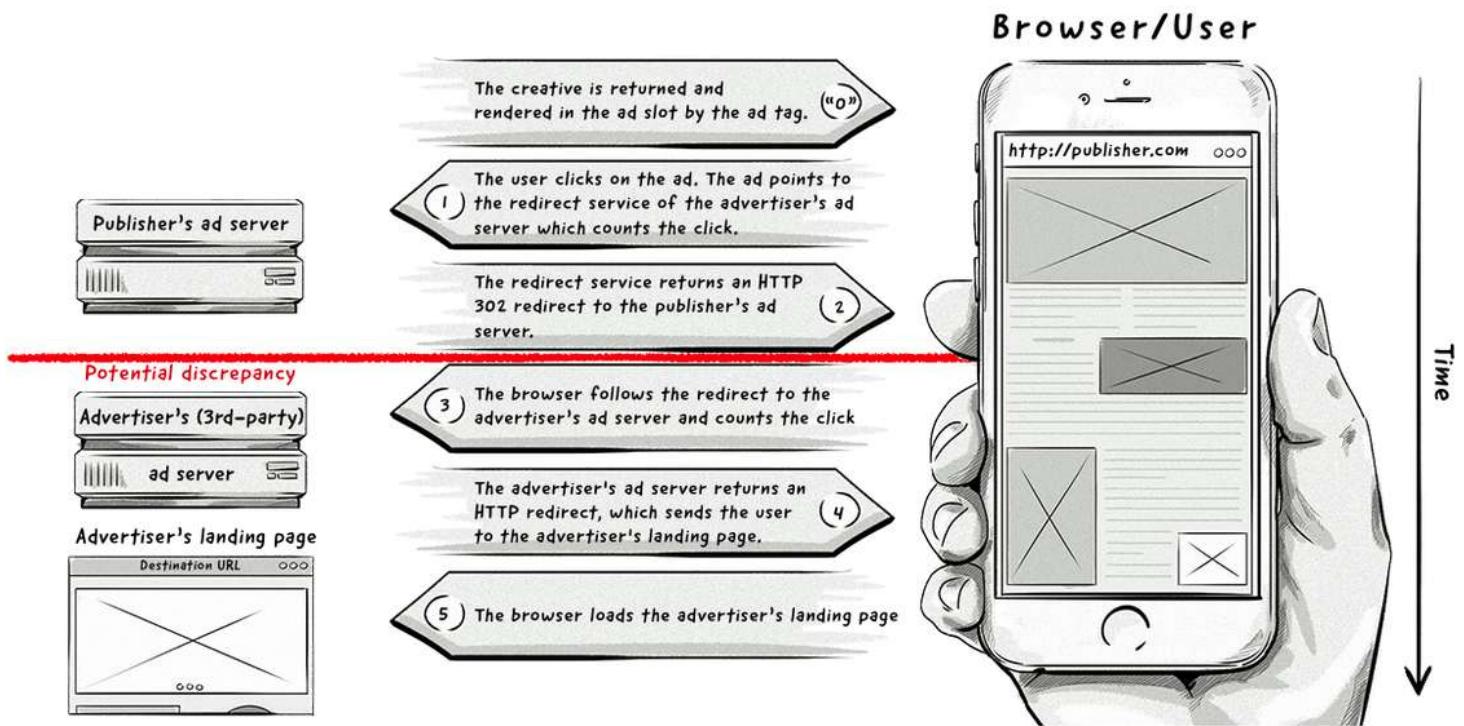
Below are two images that illustrate some situations when discrepancies are likely to occur:

1. During impression tracking:



The publisher's ad tag loads and the ad impression is tracked, but for whatever reason, the browser didn't load the advertiser's ad tag or impression pixel.

2. When counting the click:



A discrepancy could occur if the redirect chain is broken, which would mean that the advertiser's ad server wouldn't receive information about the click and the user wouldn't be taken to the final landing page.

As we can see in the above diagrams, most discrepancies will occur after the publisher's ad server has loaded the ad tag, meaning advertisers will often report lower numbers than publishers.

Discrepancies and Common Causes

Below are some possible reasons as to why discrepancies occur.

Human and Implementation Errors

AdOps are usually swamped with a lot of ad trafficking and last-minute entries. It's not uncommon for agencies to send or change tags at the last minute before the campaign goes live.

Add to this the manual work that must be performed for each of the campaigns, and it's easy to make a mistake, especially by a junior or overloaded AdOps team member.

Specifically, common errors are:

Pasting an incomplete impression-tracking pixel that's missing the full ID: Launching an incorrect pixel will result in hitting the advertiser's ad server, but not tracking the impression due to the missing ad or campaign identifier.

Using the incorrect impression pixel: For example, pasting an impression pixel from Campaign ABC to Campaign 123 that was kept in the pastebin.

Implementing the wrong macro: Failing to add a cache buster may cause the pixel to be cached by the browser and therefore won't correctly report impressions for subsequent ad views of the same user/browser.

Difference in run dates or failure to fully set up the campaign on one of the ad servers: The campaign may have already started in one ad server, but may not be running in the other ad server, which would cause the campaign to not display ads.

For example, if the tags weren't properly set up in the advertiser's ad server, but were set up correctly in the publisher's, then the publisher's tags would run properly on their site and track every impression of the empty ad.

Configuration Issues

Discrepancies in reporting can also be caused by differences in the reporting configuration between different AdTech platforms, such as:

Time zone: If one AdTech platform records events in Central Time (CT) and another one in Pacific Time (PT), then you'll notice discrepancies when looking at time-based dimensions (e.g. daily and hourly reports).

Traffic validation and filtering: Some AdTech platforms use traffic validation and filtering services in an attempt to block fraudulent traffic, which can also cause discrepancies between platforms.

Differences in terminology and counting methodology: While most AdTech platforms can agree on the proper definition of common metrics like impressions, clicks, and conversions, there can be some differences in how these are counted.

For example, one AdTech platform could count impressions when the pixel fires in the browser, whereas another could count impressions when the ad is served (i.e. when it leaves the server). In the latter case, an impression would be counted when it is served, but it might not actually load in the browser due to technical issues.

Client-Side Issues

As we mentioned above, most AdTech platforms rely on client-side tracking for reporting, but often encounter a number of technical issues, such as:

- Poor Internet connectivity and latency.
- JavaScript errors could be breaking the execution of the ad code.
- The browser could be set to disable JavaScript or use extensions like <noscript>.
- The URL's maximum length could have been reached, meaning some redirect paths could be cut off and not executed.
- Special characters passed in the URL might not be parsed correctly by the AdTech platform.
- The creative's file size could be too big or might not comply with the IAB's standards.
- The webpage could contain large files (e.g. rich images that take a long time to load), which increases overall latency.

How to Calculate an Impression Discrepancy

Calculating a discrepancy between two AdTech platforms can be done via the following formula:

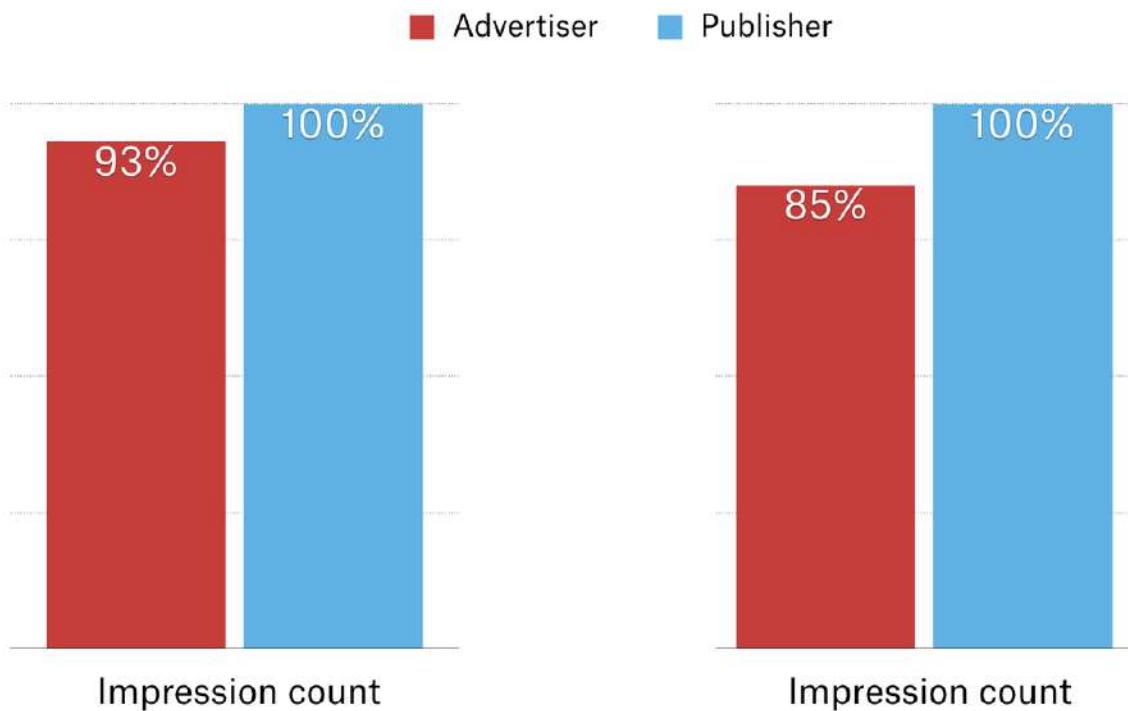
Impression discrepancy = (publisher's impression count – advertiser's impression count) / advertiser's impression count

To work out the percentage, simply multiply the final number by 100.

$$\text{Impression discrepancy} = \frac{\text{Advertiser's impression count} - \text{publisher's impression count}}{\text{Advertiser's impression count}}$$

Discrepancy Tolerance

The IAB states that a tolerance of 10% discrepancy based on the publisher's figures is acceptable.



A discrepancy is calculated from the advertiser's numbers, but if it's less than 10%, then the publisher's metric is typically used for billing.

Reconciliation

Reconciliation is a process used to compare two sets of records to ensure the figures are in agreement and are accurate.

Due to the wide-ranging number of possible reasons for discrepancies, most of the time reconciliation is a manual process whereby AdOps team members log in to their AdTech platform accounts, compile reports, download the data, and look at where the main problems lie.

Chapter Summary

- The most popular method of counting an impression is to serve a 1×1 transparent image that notifies the ad server of an impression, known as an **impression tracker** (or **impression pixel**).
- When the impression tracker loads, it records an impression in the AdTech platform.
- Tracking the number of clicks an ad receives is typically done via a **click tracker**, which is the URL of the ad server's redirect service that counts the click and redirects the visitor to the final landing page of the campaign.
- A conversion is registered every time a user completes a goal set by an advertiser or marketer, which could be a purchase or a download.
- There are two main types of conversion tracking: **click-through conversion** and **view-through conversion**, which can either be recorded by firing a pixel on the confirmation page or by tracking the conversions server-side.

- The reporting function of an AdTech platform is responsible for displaying metrics, dimensions, and subdimensions about many different areas of a campaign.
- Discrepancies, which are the difference between the reported numbers of two different AdTech platforms, are common in AdTech and there can be many reasons why they occur. Common reasons are related to human error, reporting configuration, and technical issues.
- The IAB states that a discrepancy of under 10% is acceptable.

09. Media-Buying Methods: Programmatic, Real-Time Bidding (RTB), Header Bidding, and PMP



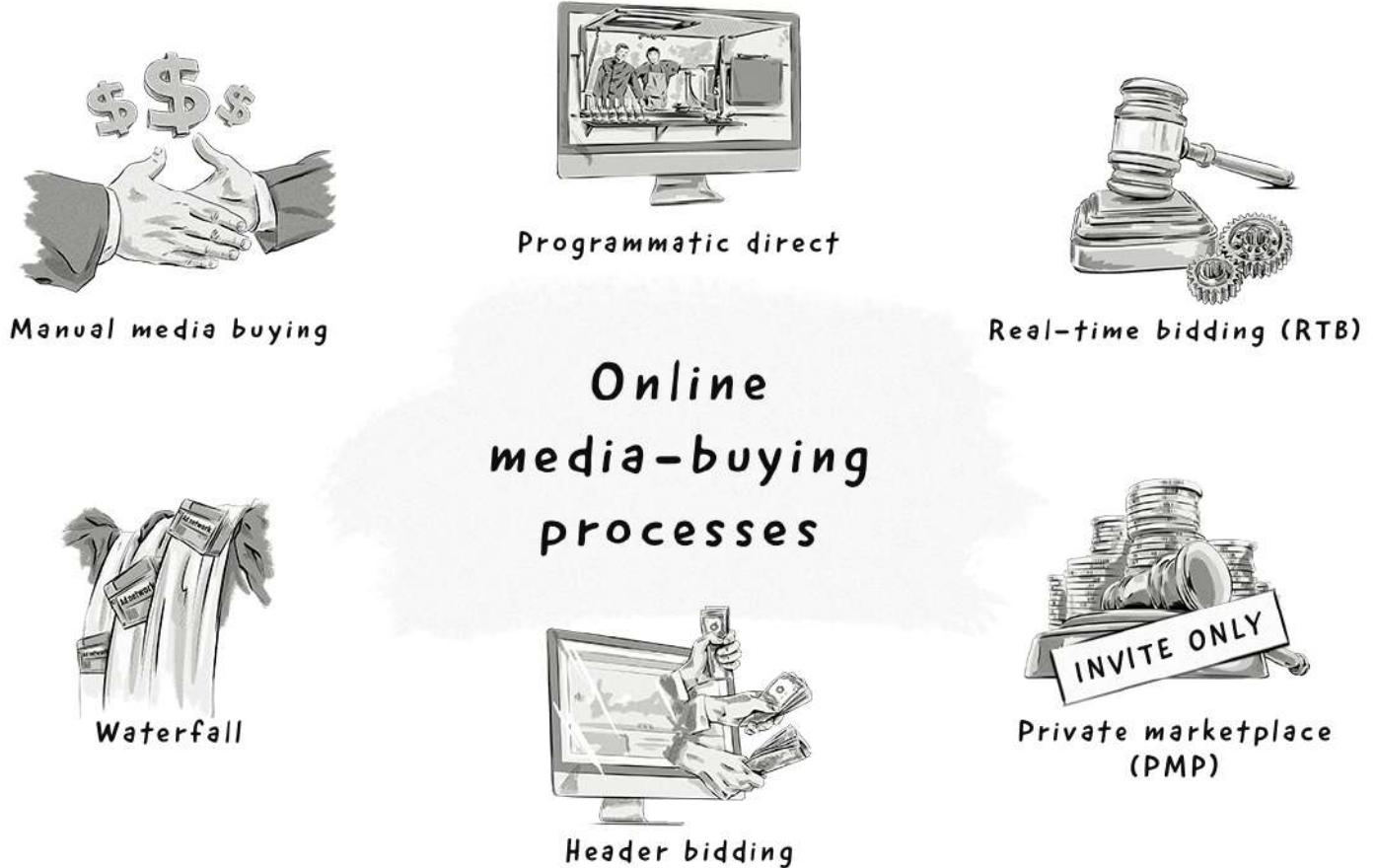
As we've covered previously in this book, the online advertising industry is made up of many advertising technology platforms, such as ad servers, DSPs, SSPs and ad networks.

The goals of these AdTech platforms vary – some are responsible for serving ads, while others are designed to help advertisers and publishers buy and sell online media.

In this chapter, we'll take a look at the media-buying processes that power these AdTech platforms.

The Main Media-Buying Processes

Below is an overview of the main media-buying processes that we'll be covering in this chapter:



Now let's take a look at these processes in more detail.

Manual Media Buying

In the early days of online advertising, the buying and selling of ads between advertisers and publishers was a very manual process.

Advertisers would work with publishers and send them ad tags directly. Because there weren't any technological platforms involved, there wasn't any way to define targeting or produce reports.

Luckily, the introduction of ad servers solved this and kickstarted the programmatic media-buying revolution.

Programmatic Media Buying

What Does Programmatic Mean?

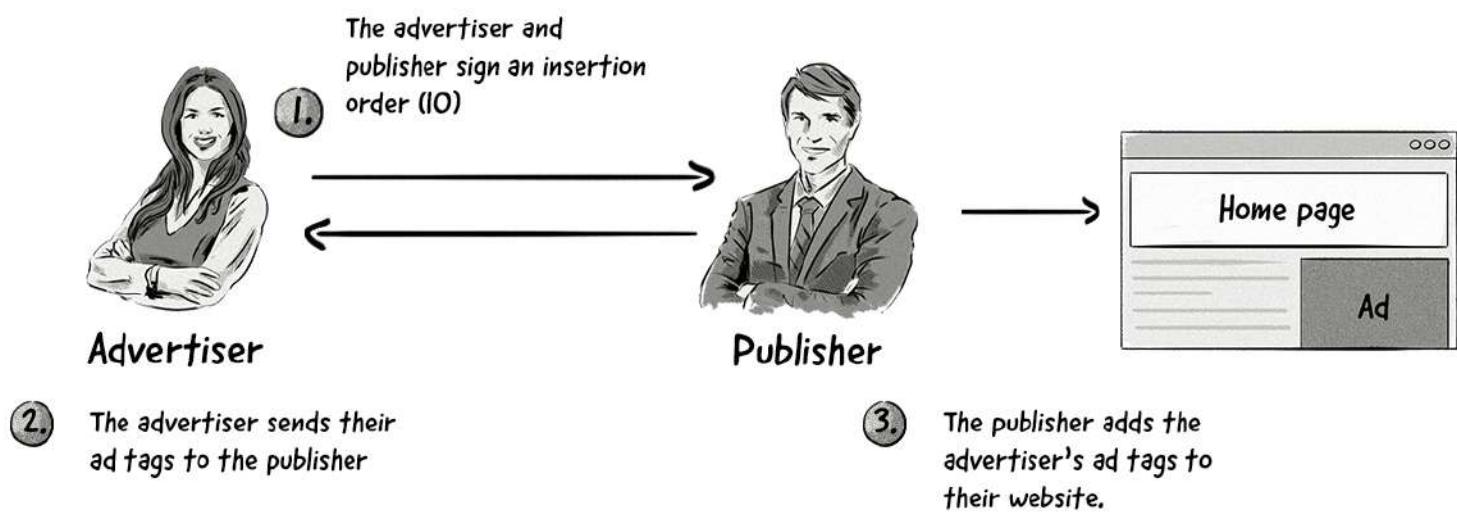
The term **programmatic** can mean different things to different people, but here's a simple and clear definition:

Programmatic refers to the use of technology, algorithms and data to buy and sell online media in an automated fashion.

Compare this to the manual way of buying advertising, which doesn't involve the use of technology or algorithms and is done human to human.

Below are some examples that illustrate the difference between the execution processes of manually purchased media and programmatically purchased media:

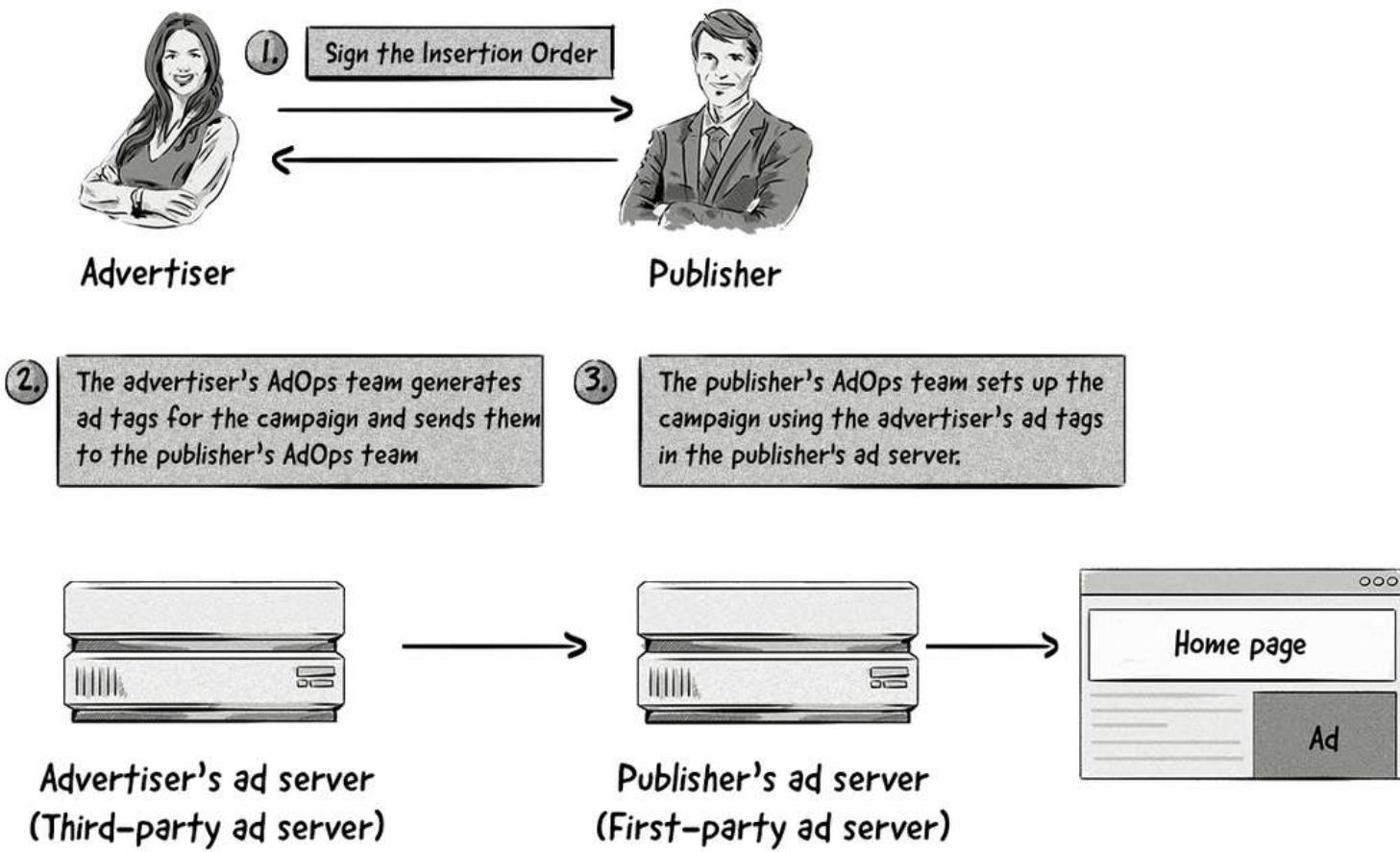
Manual media buying



The execution of a **manual** media transaction:

- The advertiser and the publisher sign an insertion order (IO), which is a contract that defines the terms and conditions of the campaign, such as flight dates and placement.
- The advertiser sends its ad tags to the publisher. These ad tags are pieces of HTML that will display the ad on the publisher's website.
- The publisher adds the advertiser's ad tags to its website and starts the campaign.

Programmatic media buying



The execution of a **programmatic** media transaction:

- The advertiser and the publisher sign an insertion order (IO), which is a contract that defines the terms and conditions of the campaign, such as flight dates and placement.
- The advertiser's AdOps team configures the campaign in the advertiser's ad server and sends the ad tags to the publisher.
- The publisher's AdOps team sets up the campaign, adds the advertiser's ad tags to the publisher's ad server and starts the campaign.

Although the above processes look similar, the main advantage of using ad servers is the added benefits they provide over manual media buying, such as targeting, placement, reporting, and the elimination of mundane and repetitive tasks.

For example, instead of a publisher adding the advertiser's ad tag on its website that would simply display the ad when the page loads, the ad tag could instead redirect to the advertiser's ad server. The benefit of this is that the ad server could then decide which ad to show the user based on a number of factors, such as location and device.

Another key difference between manually purchasing and programmatically purchasing media is the speed with which we can start and modify the campaign when it's running.

Creating and launching a campaign in a programmatic AdTech platform such as a DSP takes a matter of minutes. Without programmatic technologies, it can take several days before the campaign begins.

Also, when buying media manually without programmatic platforms, each change to the campaign has to go through the publisher's AdOps team, which can take a few days to implement. When tweaking the campaign in programmatic media-buying platforms, changes made by the AdOps are reflected close to real time.

This becomes very important, as brands have to react fast to any changes and optimizing a campaign can be done on an hourly or daily basis.

Campaign Optimization Basics: Manual vs. Algorithms

Campaign optimization involves making changes to the campaign in order to improve its performance and make media buys more economical.

There are a number of areas that can be changed in a campaign, such as the targeting criteria and the ads themselves.

Campaigns can be optimized either manually or via algorithms.

Manual optimization

Manual optimization typically involves advertisers adjusting their CPC, CPA and CPM bids, usually on a daily basis.

Basically, an advertiser uses data broken down by all the different dimensions provided by the ad platform, such as geolocation, gender, interests, device type, etc., and uses those dimensions to extend or limit targeting to specific groups.

By doing so, the advertiser creates very specific targeting criteria that provides the most optimal CTR, CPA or conversion rate.

In order to make the optimizations, advertisers utilize data to determine which bids to adjust, including:

- The ads' CTRs
- The number of clicks generated by the ads
- The number of impressions generated by the ads

Below is a process media buyers could use to manually optimize a campaign:

- Start by breaking down the data by one or more dimensions, such as geolocation, device, publisher domain, time of day, carrier, etc.
- Filter out non-significant data. For example, only ads that generate a few impressions or clicks, or filter by significant data, such as ads that generate the most impressions or clicks.
- See the best- and worst-performing values, such as device type or geolocation.

- Also, you could view certain metrics, depending on what you want to optimize. Examples could include the effective cost per mille (eCPM) of an ebook download or something lower in your sales or marketing funnel, such as cost per qualified lead.
- Blacklist the areas (i.e. exclude from targeting) that are underperforming or not performing at all.

There are a number of other techniques an advertiser could use to optimize a campaign, including:

- **Running A/B tests:** Making changes to the creatives and running tests to see which variant performs better.
- **Personalizing the creatives (dynamic creatives):** Changing the messaging or visual aspects of the creatives to make them more relevant for different segments. Examples can include adding a city name to the creatives so that it matches the user's location.
- **Experimenting with different traffic sources:** Seeing how different sources (e.g. websites), mediums (e.g. display and video ads) and AdTech platforms perform by experimenting with a small percentage of an advertiser's budget (5-10%) and compare metrics like the eCPA, eCPM, etc., against one another.

Automated optimization

Automated optimization involves using algorithms to power the optimization process.

Many AdTech platforms have built-in algorithms that deliver some sort of automated optimization functionality.

The key component of successful automated optimization is historical data. The algorithms are only able to make decisions and optimizations if they have the proper amount and quality of data to fuel them.

Programmatic Direct

Programmatic direct (aka programmatic guaranteed, programmatic reserved, automated guaranteed) is a method of buying and selling media, but unlike RTB, no auctions are held.

Instead, an advertiser and publisher agree on the inventory and the CPM, then the rest of the process is handled programmatically via the use of AdTech platforms.

Programmatic direct is very similar to the way media was bought and sold prior to the Internet and even in the early days of online advertising, but provides more scale thanks to the use of advertising technology.



The programmatic-direct process is similar to placing an order on an ecommerce platform, but instead of buying a product, you are buying media inventory.

The process looks like this:

- An advertiser browses through catalogs of websites.
- It chooses placements, flight dates and the volume of impressions.
- It configures creatives and additional tracking pixels.
- It places an order on the platform.
- The publisher audits and verifies the campaign.
- The order is executed without additional involvement from the AdOps team, except for an audit, which it carries out.

The main advantage of programmatic direct is the ability to secure premium inventory at a premium price.

Although programmatic direct means advertisers may need to pay higher CPMs compared to other media-buying processes (such as RTB), they are able to secure premium inventory before the ad space is offered on an open RTB auction. This allows them to reach their target audience when they otherwise might not have been able to.

For publishers, this results in higher CPMs.

The main disadvantage of programmatic direct for advertisers is that there are less targeting options available, as they are simply displaying ads based on the context and known audience of a website.

For example, a bank could show an ad about its new bank account on a financial website.

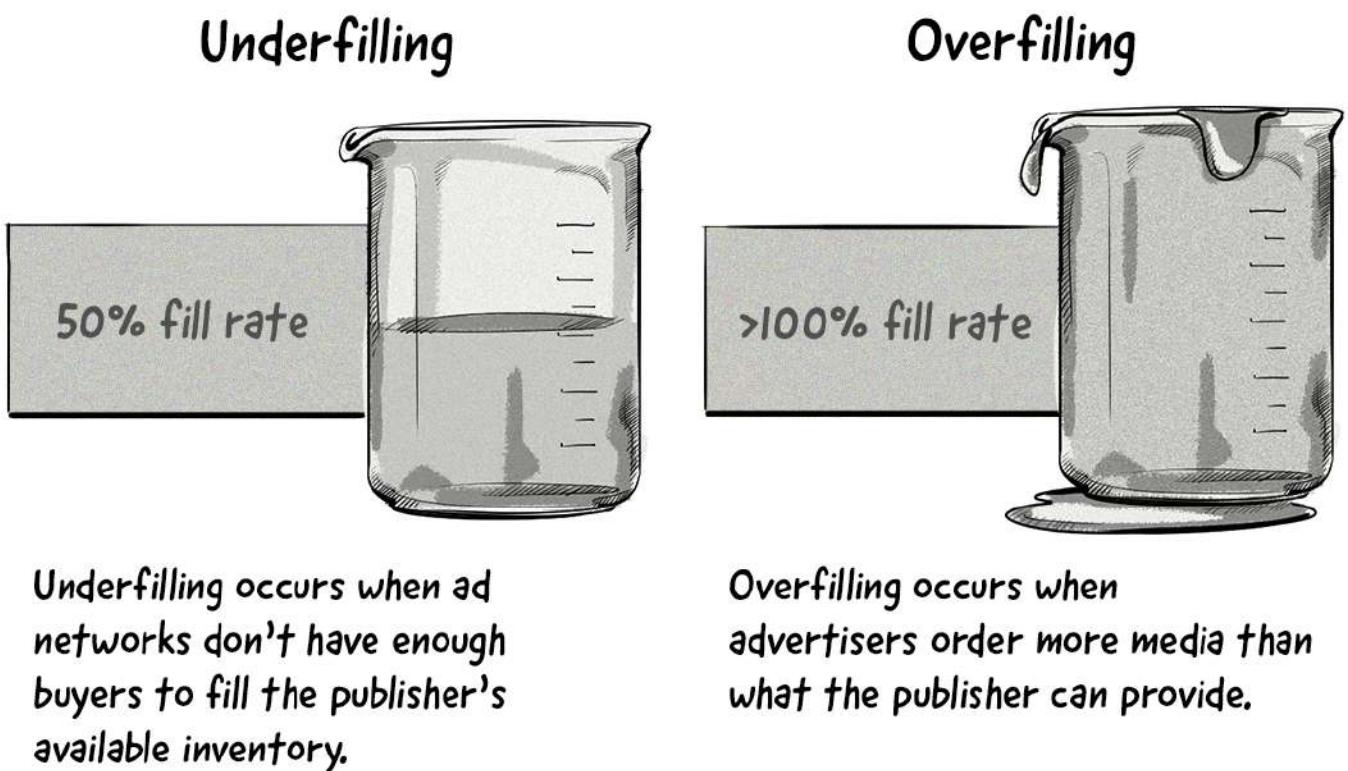
Compare that to RTB, where the same bank could show the same ad across many different websites only to people who had visited its website.

For publishers, the main disadvantage is that they may not be able to sell all of their inventory via programmatic direct. However, many publishers set up a waterfall to ensure they sell as much inventory as they can. More on this below.

Real-Time Bidding (RTB)

The mid-to-late '90s saw a number of ad networks emerge, so much so that by the mid-2000s there were hundreds of ad networks on the market.

However, ad networks soon found themselves falling victim to either **underfilling** or **overfilling** ad campaigns.



Publishers soon realized that their ad network wasn't selling all of their available inventory, so they started working with more ad networks. However, this meant adding more tags to their websites, which lead to latency issues and a poor user experience.

To combat the latency issues, a new type of platform emerged, **supply-side platforms (SSPs)**, originally referred to as **network optimizers**.

The first supply-side platforms (SSPs)

The first SSPs to hit the market were Collective, [Pubmatic](#), [Admeld](#), and [Magnite](#) (formerly The Rubicon Project).

Instead of adding multiple tags to a website, publishers included just one tag that redirected to an SSP.

From there, the SSP worked out which ad networks were interested in purchasing the publisher's inventory and then finalized the transaction.

The mid-to-late 2000s not only saw the rise of SSPs, but also [**demand-side platforms \(DSPs\)**](#).

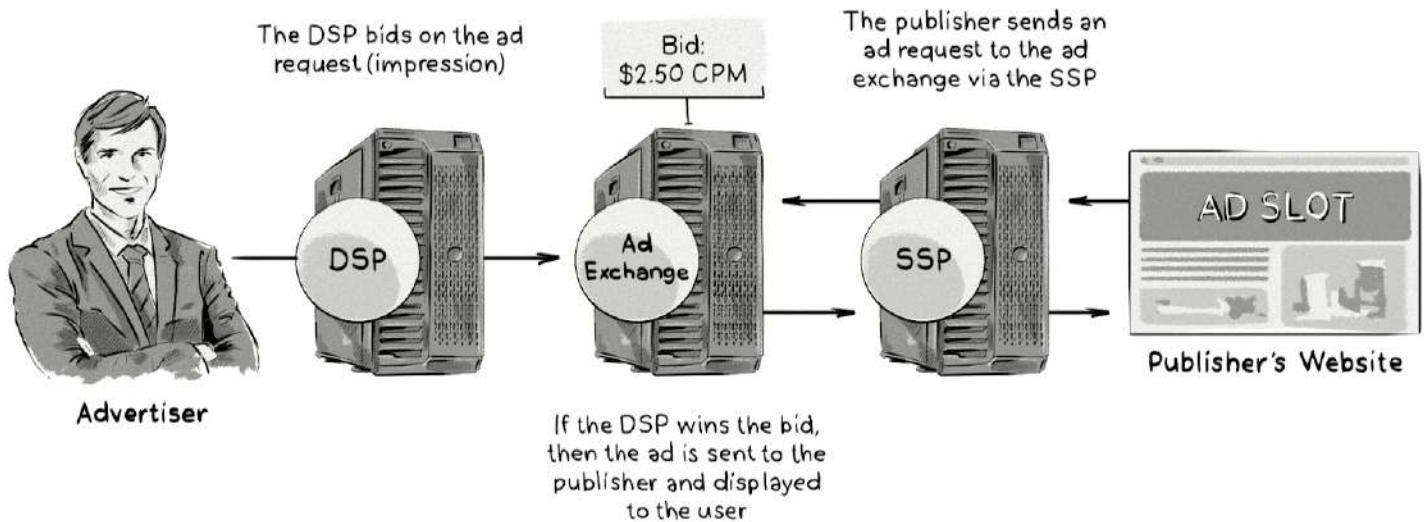
DSPs emerged as a way for media buyers (advertisers and agencies) to connect to publishers' inventory offered through SSPs.

The first demand-side platforms (DSPs)

The first DSPs that emerged were Invite Media (now part of the [Google Marketing Platform](#)), [dataxu](#), and [MediaMath](#).

Around the same time, the next revolutionary AdTech platform to hit the online display advertising industry was the [ad exchange](#).

Ad exchanges emerged as a way to help solve the liquidity issues by auctioning off a publisher's inventory on an impression-by-impression basis.



The ad exchange handles the buying and selling of media between an advertiser and publisher.

The easiest way to explain how **ad exchanges** operate is to compare them to the stock exchange.

In the same way stock exchanges facilitate the buying and selling of stocks, bonds and other securities, ad exchanges handle the buying and selling of ad impressions between advertisers and publishers in real time.

Did you know?

In 2007, the three largest ad exchanges – DoubleClick, AdECN and RightMedia – were all bought by Google, Microsoft, and Yahoo! respectively.

This ability to buy and sell individual impressions in real time is known as **real-time bidding (RTB)**.

What Is Real-Time Bidding (RTB)?

Real-time bidding (RTB) is a protocol that was introduced in the late 2000s and was a big game changer for the way online media was bought and sold.

Originally designed to help publishers sell remnant inventory to advertisers, RTB is now used to sell all types of inventory, including premium inventory.

Instead of buying thousands of impressions from the same publisher, RTB allows advertisers to purchase individual impressions across multiple publishers to reach their target audience more precisely and bid based on the information known about the website and user at that particular time.

Publishers also benefit by receiving higher CPMs for their inventory.

What is the RTB Project (OpenRTB)?

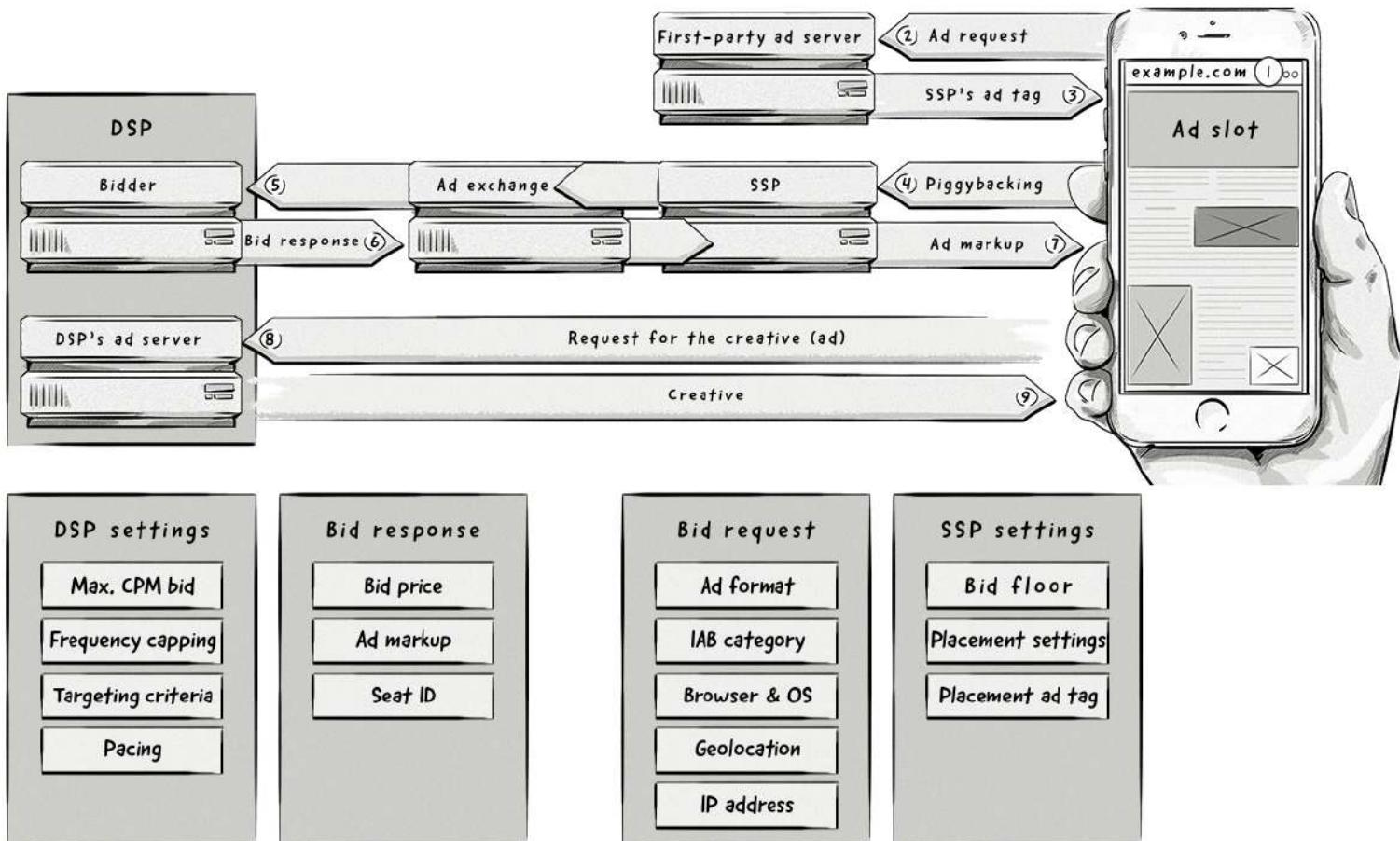
The RTB Project, formerly known as the OpenRTB Consortium and now referred to as [OpenRTB](#), is a group led by the Interactive Advertising Bureau, consisting of AdTech companies from both the demand and supply sides.

Started in November 2010, OpenRTB provides AdTech vendors with an API specification. This protocol (known as the OpenRTB protocol) allows platforms to communicate between one another using a common language to buy and sell digital media.

How Does RTB Work?

The technical side of RTB is highly complex and involves multiple AdTech platforms.

Below is a detailed illustration and description of how the RTB ad exchange works.



A detailed look at how the RTB process works.

- A user visits a page (example.com).
- The page contains an ad slot with JavaScript code that requests content from the first-party ad server, known as an ad request. The request also passes additional data about the user, such as their location, device type and operating system.
- The ad server checks if there are any direct campaigns matching the user. If not, the ad server returns the SSP's ad tag, which will offer the impression on an RTB auction.
- The browser loads the script contained in the SSP ad tag from the server. User information and placement details like page URL, size, and restrictions are passed to the ad exchange.
- The ad exchange announces the available ad impression to all bidders via a bid request.
- Bidders evaluate the bid request and match targeting parameters, such as page domain, context, location and other data collected about the user. They then place their bids – basically, they state how much they want to pay for this impression, if anything. They also send the markup of the ad that they would like to display. The bid price and ad markup are enclosed in an object called the bid response.
- The ad exchange receives the bids and the impression goes to the highest bidder. The highest bidder pays the price of the second-highest bid, plus an additional small amount (usually \$0.01). This is known as a second-price auction. A win notice containing the final price sends from the ad exchange to the winning DSP, which is done via a server-to-server request or through the ad markup via a pixel with a price macro that's filled in automatically by the ad exchange. The winning DSP's ad markup is sent to the browser.

- The DSP's ad markup loads in the browser and sends a request to retrieve the creative (ad) from the DSP's ad server. It is quite common for the ad markup to request the creative from a content-delivery network (CDN) instead of directly from the ad server. An impression-tracking pixel also fires, which notifies the ad server that an impression has been served.
- The DSP's ad server sends the creative to the browser and the ad displays to the user.

This entire process happens in real time when an ad is loaded onto the page, usually **within 100–150 milliseconds**. To put that in perspective, it takes about **300 milliseconds to blink!**

Each time a page is loaded or refreshed, a new ad request is sent from the page, which subsequently starts a new RTB auction.

What Information Do Bid Requests and Bid Responses Contain?

Bid requests and bid responses typically use JavaScript Object Notation (JSON) format for its human readability and compactness.

Here's an example of part of a bid request from the [IAB's OpenRTB 2.5 specification](#):

```
{
  "id": "80ce30c53c16e6ede735f123ef6e32361bfc7b22",
  "at": 1,
  "cur": ["USD"],
  "imp": [
    {
      "id": "1",
      "bidfloor": 0.03,
      "banner": {
        "h": 250,
        "w": 300,
        "pos": 0
      }
    },
    ],
    "site": {
      "id": "102855",
      "cat": ["IAB3-1"],
      "domain": "www.foobar.com",
      "page": "http://www.foobar.com/1234.html",
      "publisher": {
        "id": "8953",
        "name": "foobar.com",
        "cat": ["IAB3-1"],
        "domain": "foobar.com"
      }
    },
    "device": {
      "ua": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/537.13 (KHTML, like Gecko) Version/5.1.7 Safari/534.57.2",
      "make": "Apple",
      "model": "iPhone",
      "ip": "123.145.167.10"
    },
    "user": {
      "id": "55816b39711f9b5acf3b90e313ed29e51665623f"
    }
}
```

Here's an example of a bid response:

```
{  
  "id": "1234567890",  
  "bidid": "abc1123",  
  "cur": "USD",  
  "seatbid": [  
    {"seat": "512",  
     "bid": [  
       {"id": "1",  
        "impid": "102",  
        "price": 9.43,  
        "nurl": "http://adserver.com/winnnotice?impid=102",  
        "iurl": "http://adserver.com/pathtosampleimage",  
        "adomain": ["advertiserdomain.com"],  
        "cid": "campaign111",  
        "crid": "creative112",  
        "attr": [1, 2, 3, 4, 5, 6, 7, 12]  
      ]  
    ]  
  ]  
}
```

The OpenRTB specifications list dozens of objects (e.g. BidRequest, Source, and Device) and object attributes.

These objects and object attributes help DSPs decide whether an impression is worth bidding on and relay other pieces of information to the advertiser via the DSP.

Here's a list of some of the main OpenRTB objects and their attributes:

Imp (impression)

- id
- banner
- video
- audio
- native

Banner

- w (width)
- h (height)

Video

- minduration (minimum duration of video ad)
- maxduration (maximum duration of video ad)
- skip (denotes whether the ad can be skipped)

There are other objects for audio, native and in-app mobile ads.

Publisher

- id
- Name
- Domain

Device

- ua (user agent)
- geo (location)
- devicetype
- make
- model
- os (operating system)
- language
- carrier

Geo

- lat (latitude)
- lon (longitude)
- country
- region
- city
- zip

User

- id
- yob (year of birth)
- gender

Data

- id
- name
- segment

Segment

- id
- name
- value

For a detailed list of the different objects and attributes, view the OpenRTB [2.5](#) and [3.0](#) specifications.

The Benefits of RTB for Advertisers and Publishers

For Advertisers

Increased ad effectiveness: Advertisers are able to view the results of their campaigns in real time and make changes to them to improve performance. These changes can be made manually by the advertiser or by a DSP's algorithms.

Fraudulent-inventory recognition: Because advertisers have real-time campaign reports, it's easier to detect fraudulent activity, such as extremely high click-through rates. Many RTB platforms incorporate ad-fraud prevention and detection software to help advertisers reduce ad waste.

For Publishers

Increased revenue: RTB opens a publisher's inventory to dozens, even hundreds, of advertisers, which results in better campaign matching and higher CPMs.

Optimized price floors: In the same way advertisers use real-time analytics to improve their campaigns, publishers can also use real-time analytics to adjust their inventory's CPM floor price to increase revenue.

Transparency Issues Regarding Commissions and Viewability in the RTB Ecosystem

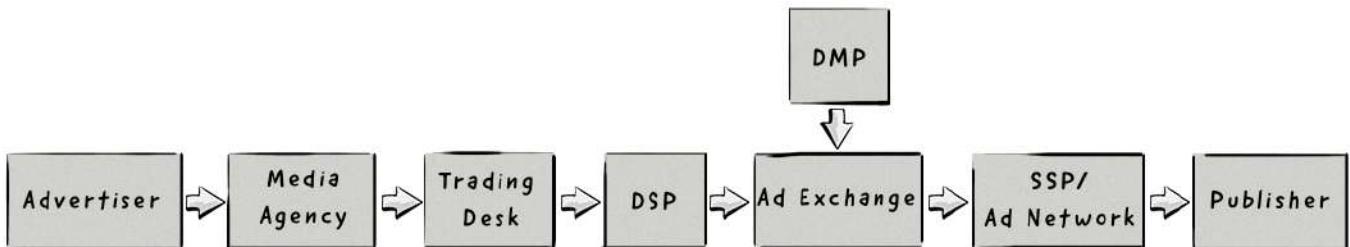
Back in the day when the movement of media between the advertiser and publisher was a purely direct process, both parties knew how much the media was being sold and purchased for.

While this direct process is still occurring today, the benefits offered by technology platforms (DSPs, SSPs, DMPs, etc.) are leading to an increase in programmatic media buying for both remnant and premium inventory.

However, even though these platforms are providing advertisers and publishers with an easier and more optimized way of buying and selling media, they have essentially become the middlemen and are making the true cost of media harder to identify.

When an advertiser makes a media purchase with its agency, it is often unaware of how many hands its budget passes through, and how many commissions are paid to the intermediaries and technology platforms before it reaches the user.

It is not uncommon for an ad to pass through five different parties before it reaches the publisher. That's up to five middlemen all taking different commissions and charging their own fees.



Intermediary Commissions and Fees

Knowing exactly how much commission each technology platform takes (DSP, Ad Exchange, SSP) is extremely hard to calculate, and even if this information is passed on to the advertiser, it can be more difficult to validate and confirm.

However, a 2020 report by PwC and the Incorporated Society of British Advertisers (ISBA) titled the [Programmatic Supply Chain Transparency Study](#) found that, on average, publishers received just 51% of ad spent, with 35% going to the intermediaries, e.g. ad agencies and AdTech companies. The report also found that 15% of that ad spend, known as the unknown delta, couldn't be accounted for.

Some of the key highlights from the report are:

- Demand-side tech fees, such as ad serving, verification tools and data, averaged to account for 10% of advertiser spend.
- SSP fees worked out to be, on average, 14% of publisher revenues, which is equivalent to about 8% of advertiser spend.
- The percentage of ad spend that publishers receive ranged from 49% to 67%.

A 2014 industry study conducted by PwC and [sponsored by the IAB](#) also found that around 50% of an advertiser's media budget went to fees and commissions.

We consistently heard throughout our conversations with industry executives that programmatic ad tech fees are substantial – generally close to 50% or more. These ad tech fees were often referred to as the “ad tech tax” in our conversations. Ad tech tax in this context refers to the fees imposed on buyers and sellers for leveraging ad tech technology, and/or value adds from ATDs, DSPs, SSPs, ad servers and ad networks. In many instances, these fees get compounded as fees from one supplier get added to the costs of the next supplier in the programmatic value chain.

[1] IAB Programmatic Revenue Report 2014 Results: An industry study conducted by PwC and sponsored by the Interactive Advertising Bureau (IAB). July 2015.

The study went on to state that the percentage varies among companies and may be lower depending on the number of AdTech platforms an advertiser uses to run media campaigns.

For example, an advertiser using just one DSP to purchase media through an ad exchange would likely pay fewer fees than one who uses an ad agency, which uses an ATD and DSP to purchase media from an ad exchange.

In the current programmatic system, advertisers are only informed about the price of the media in relation to the quantity (e.g. \$10 for 1,000 impressions = CPM), but they have no way of finding out what percentage of that will be taken by the technology platform and what percentage the publisher will actually receive.

In addition to the main platforms and intermediaries, advertisers may also pay for third-party data (e.g. behavioral and demographic verification data) from a data-management platform (DMP) as well as additional services (viewability, brand-safety verification, etc).

While the cost of the data is usually known to the advertiser, the DSP may add some hidden margins to its price.

Where Does the Industry Go From Here?

There is no doubt that lack of transparency is an issue that needs immediate attention. One way to start is to educate advertisers on the inner workings of various technology platforms and highlight the value they provide.

Thankfully, many AdTech vendors are becoming more transparent about their fees and commissions.

Private Marketplace (PMP)

Although RTB helped publishers sell their remnant inventory on the open market, many premium publishers found that they were losing money on their most premium inventory.

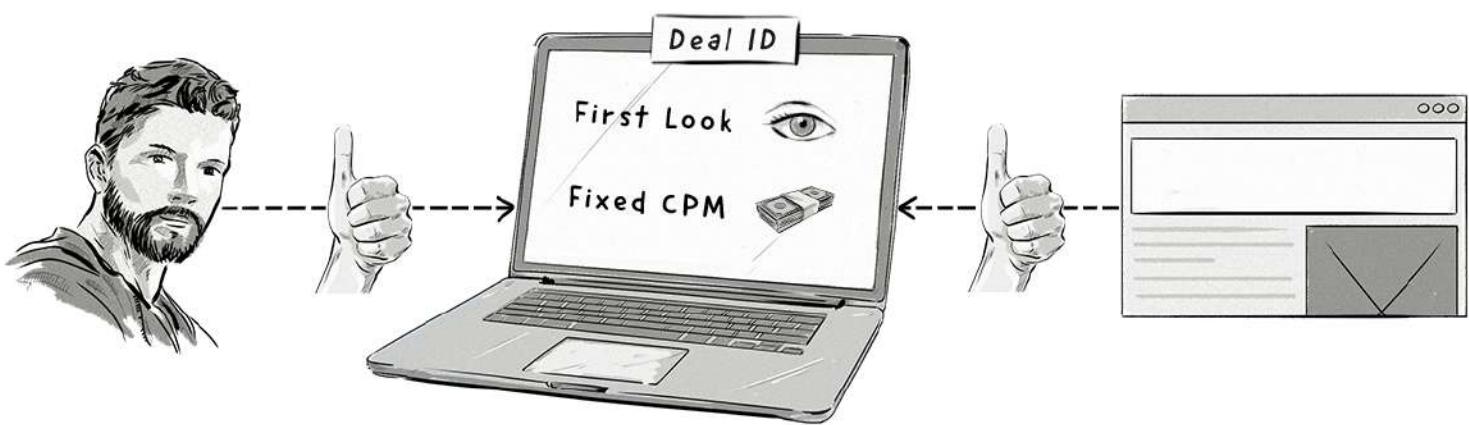
Advertisers also became concerned that they were missing out on premium inventory and their ads weren't even seen by visitors.

To overcome these issues, private marketplace (PMP) was born.

Private marketplace is an invite-only variation of the RTB model where publishers offer their most premium inventory to a select number of buyers.

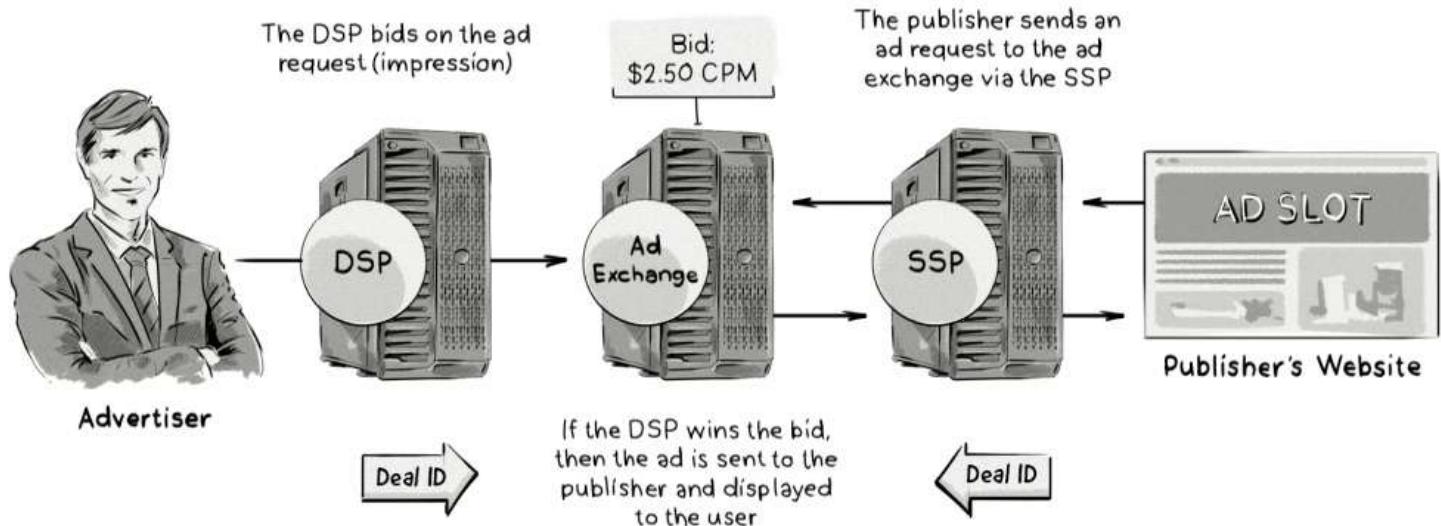
Advertisers participating in PMP deals can bid on the available inventory before the publisher offers it in an open RTB auction.

Pre-negotiated / Preferred deal



Even though the CPM is higher than in public RTB auctions, advertisers buying inventory on a PMP have first access to a publisher's premium inventory before it's sold on public auctions or via other avenues.

Publishers mark their PMP inventory by passing a ***Deal ID*** in the bid request. In order for advertisers to purchase this inventory, they must have a matching ***Deal ID***.



A Comparison Table of the Above Media-Buying Processes

Below is a comparison table that illustrates how the three ways of purchasing media stack up against each other.

Media Execution Type	Programmatic			Non-Programmatic (Direct Campaigns)	
	Real-Time Bidding (RTB)		Programmatic Direct		
	Public Auctions	Private Marketplaces (PMP/Deal ID)			
Price	Auction	Auction and/or Deal ID terms	Pre-defined	Pre-defined	
Direct Advertiser-Publisher Relationship	No	Yes	Yes / limited	Yes	
Inventory Volume	Non-guaranteed	Non-guaranteed	Guaranteed	Guaranteed	
Inventory	All inventory that the	Premium inventory	All, including	All, including	

	publisher decides to put on public auction		premium inventory Bulk inventory (sometimes robust targeting is available)	premium inventory Bulk inventory with limited targeting
Delivery	DSP / over RTB pipes	DSP / over RTB pipes with Deal ID set	Programmatic-direct platform integrated with the publisher's ad server	Email/phone, manual ad tags entered in the publisher's ad server
Advantages	<ul style="list-style-type: none"> • Per-impression buying process • Advertisers and publishers use a single dashboard • Easy testing and adjusting • Insights • Ability to sell remnant ad space 	<ul style="list-style-type: none"> • Transparency of purchased inventory and pricing • Programmatic efficiency without middlemen • Becoming an industry standard • Can remove the need for a direct-sales team 	<ul style="list-style-type: none"> • Transparency • Automation • Better insights and control • Directness • Guaranteed inventory volume 	<ul style="list-style-type: none"> • Transparency • Direct advertiser-publisher relationship • Insights and better control • Guaranteed inventory volume
Disadvantages	<ul style="list-style-type: none"> • Limited access to premium inventory 	<ul style="list-style-type: none"> • More expensive inventory 	<ul style="list-style-type: none"> • Direct deals and pre-defined prices may lead to overpaying for inventory 	<ul style="list-style-type: none"> • Not easily scalable • Slow process

The table above shows the types of media execution for real-time bidding, programmatic direct and private marketplace.

Now that we've covered the main ways media can be bought and sold, we'll look at two processes that publishers can use to manage and organize the above media-buying methods.

The Publisher's Waterfall

Waterfalling, also known as a **daisy chain** or **waterfall tags**, is a process used by a publisher to sell all remnant inventory. This process occurs when a publisher has been unable to sell its premium ad slots that are usually reserved for direct ad sales between the publisher's internal sales team and advertisers.

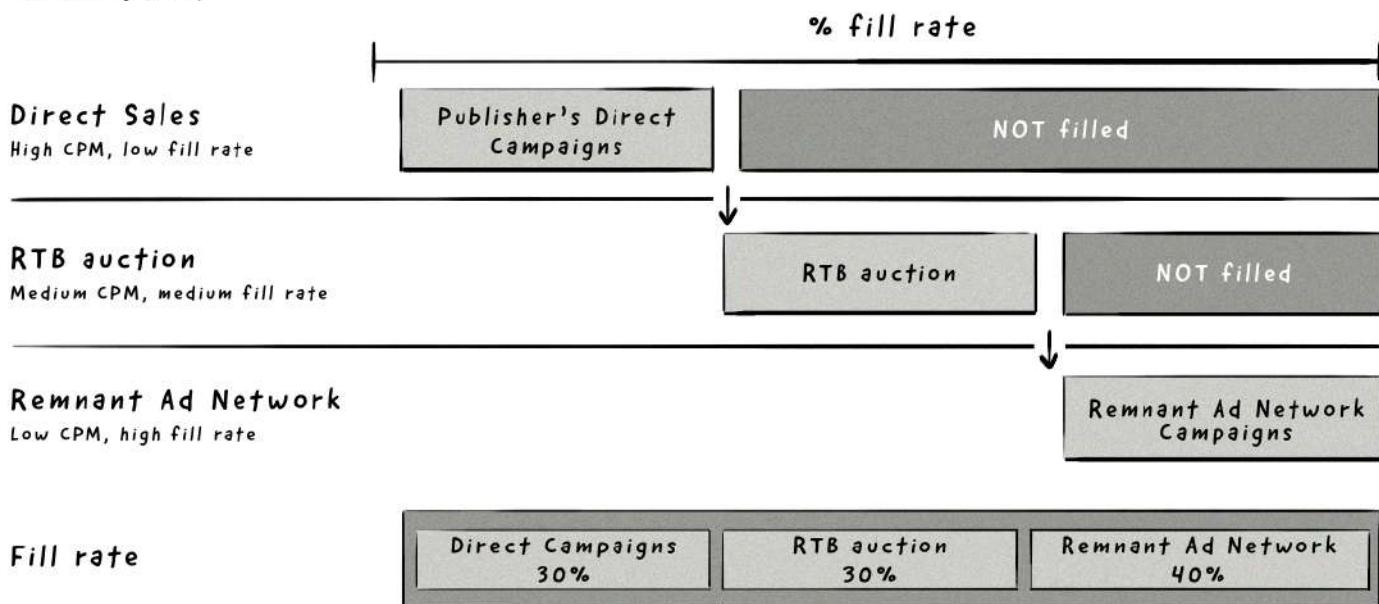
Waterfalling gets its name from the waterfall-like process for selling inventory; the demand sources are initiated one at a time, one after another.

The advantage of this daisy chain is that the publisher is able to sell off its inventory; however, as the impressions go further down the waterfall, the CPM price, which is worked out as an average, decreases.

The Publisher's Dilemma: High CPM or High Fill Rate?

While ad networks allow publishers to sell their remnant inventory, they still face what's known as the publisher's dilemma – should they **sell their inventory at a high CPM** and risk not filling all of their available ad slots, missing out on revenue opportunities? Or should they **fill all of their inventory** and receive less CPM for their ad slots, missing out on potentially higher revenue opportunities?

- Making money
- NOT making money



The image above illustrates the risks and rewards of selling inventory on different ad networks.

In the image above, we can see the publisher first tries to sell its inventory via direct sales, as these generally offer the highest cost-per mille (CPM).

If it is unable to do so, the publisher will then pass the impression to SSPs and ad exchanges and aim to sell the impression in an open RTB auction. If the ad space is still unsold, it will pass the impression to an ad network.

How Is Waterfalling Implemented?

The AdOps team sets up an ad network with a tracking tag that will execute if and when an impression is not filled.

This is typically configured in the publisher's ad server as well as in each ad network's system that the publisher works with in a field called *Fallback Ads*, *Passbacks*, *Redirects*, *Default Ads*, or similar.

These passbacks will need to be configured for each ad network used by the publisher. Referring to the image above, the publisher's AdOps team would configure the **premium ad network** to "passback" to the **remnant ad network**.

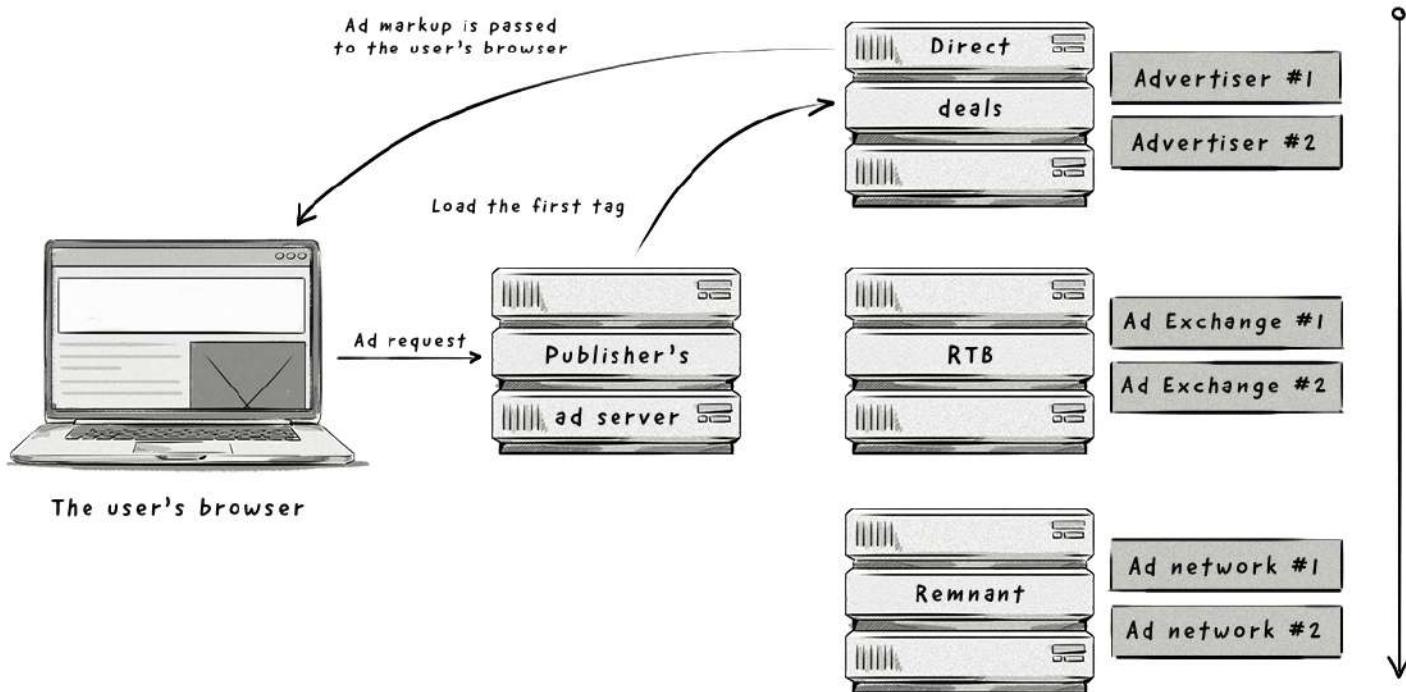
How Does Waterfalling Work?

If a publisher is unable to sell its direct buys, its ad server executes the first ad network's tag.

There are a couple of possible outcomes, so let's take a look at a few likely scenarios.

Scenario 1

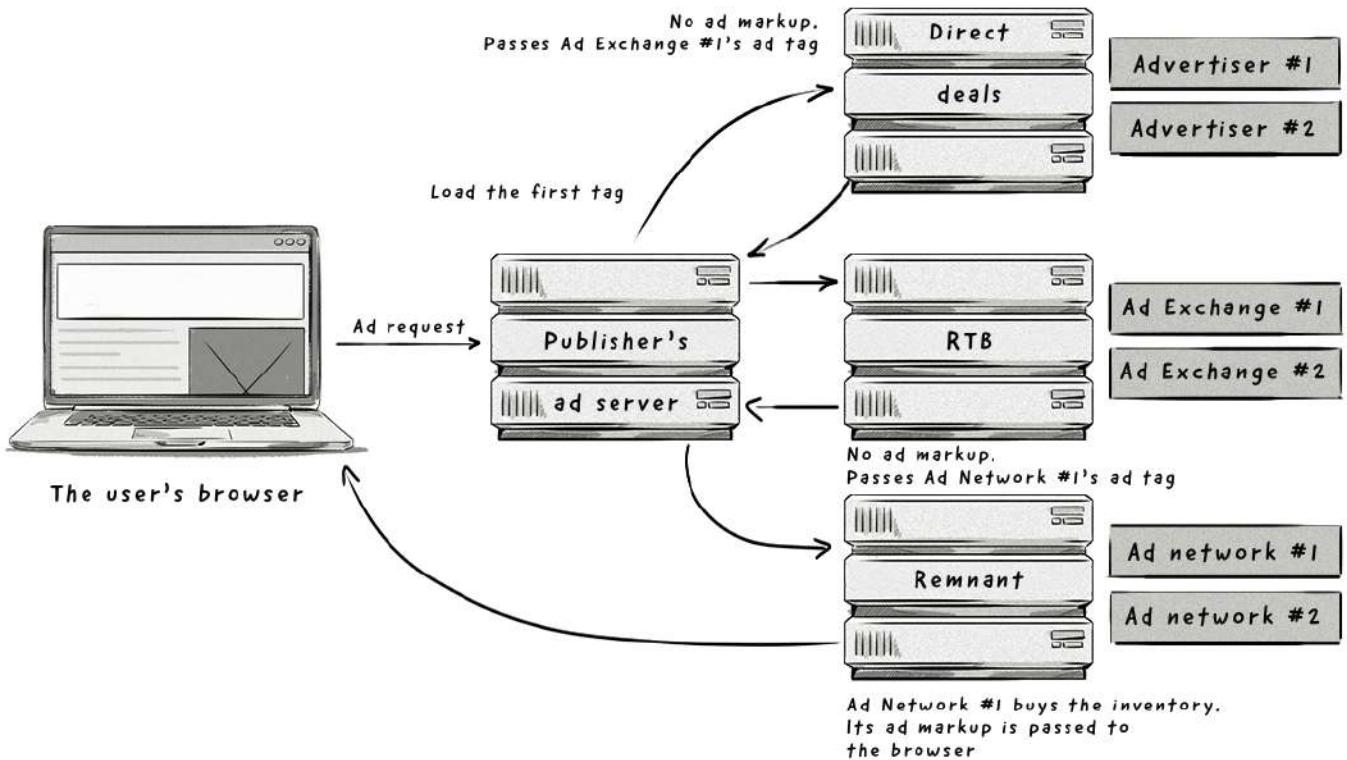
A direct deal with advertiser #1 is able to offer an impression for this ad call, so it sends an ad back to the user's browser.



Scenario 2

The publisher's **direct deals** doesn't have an impression to offer, so it loads the tag to hold **RTB auctions with ad exchange #1 and #2**, which also don't have an impression to offer, so it loads the ad tag for **remnant ad networks #1**, which is able to offer an impression for this ad request.

The impression is then sent to the user's browser and the ad is displayed.



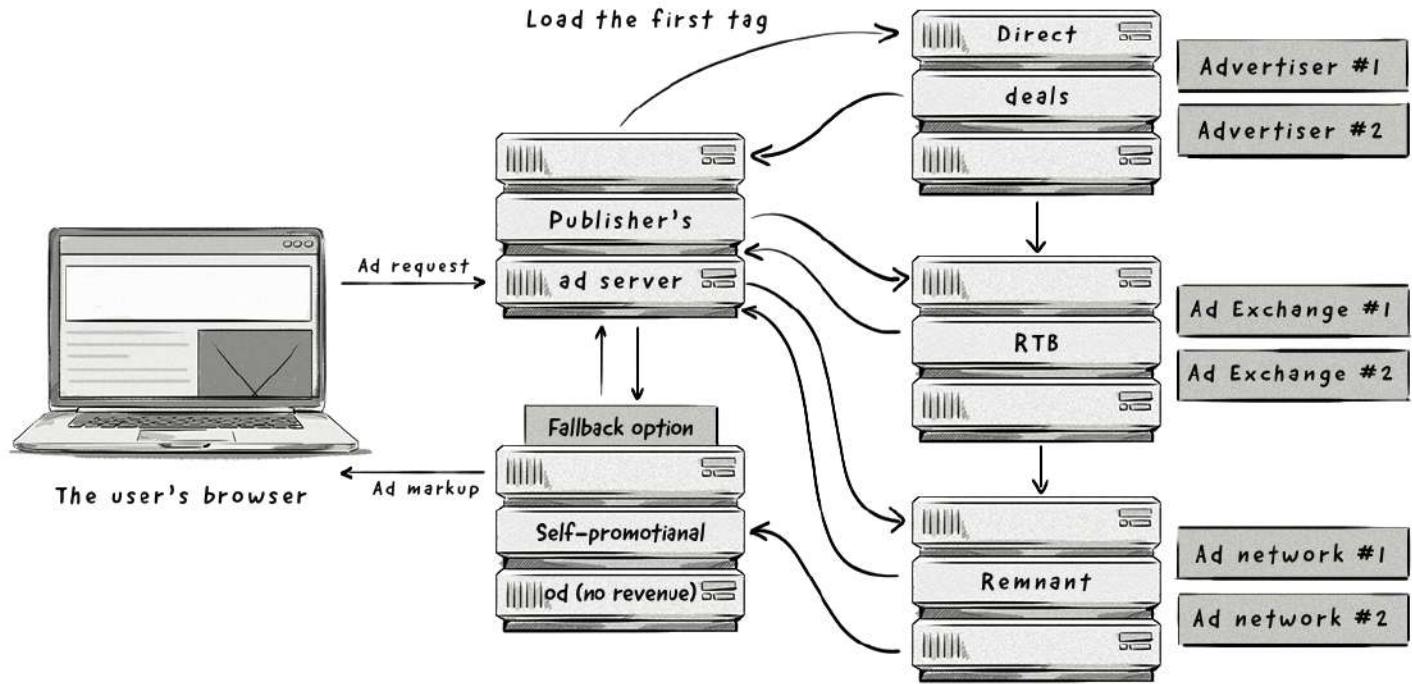
Why didn't any of the direct deals or RTB sources buy the inventory?

There are a couple of possible reasons why these two sources didn't return an impression. These include:

- **No matching campaigns:** It's possible that the advertiser's targeting criteria might not have matched the website or user, meaning the demand source (ad network or DSP) wouldn't have had a suitable ad to display.
- **High floor price:** The publisher's high floor price might have been higher than what the advertiser was willing to pay.
- **Impression capping:** Advertisers set up impression capping to limit the number of times an ad is shown to a given user, so it's likely that the ad may have reached its maximum number of impressions for that given timeframe.
- **Timed out:** Another reason is that the advertiser's ad server, ad network or DSP may have taken too long to respond to the ad request, meaning it was timed out. If this happens, it wouldn't send back the passback ad tag, meaning the waterfall would end and no ads would be displayed. This situation is one of the main downsides of using the waterfall option.

Scenario 3

If all the demand sources don't offer an impression, the publisher activates its fallback option. In most cases, this is an ad promoting its own products or services.



How Does the Ad Server Know Which Ad Network to Load First?

Publishers typically set up a ranking system whereby the demand sources are placed from highest average historical yield to the lowest.

The average historical yield is simply the average amount of revenue the demand source has made for the publisher in the past.

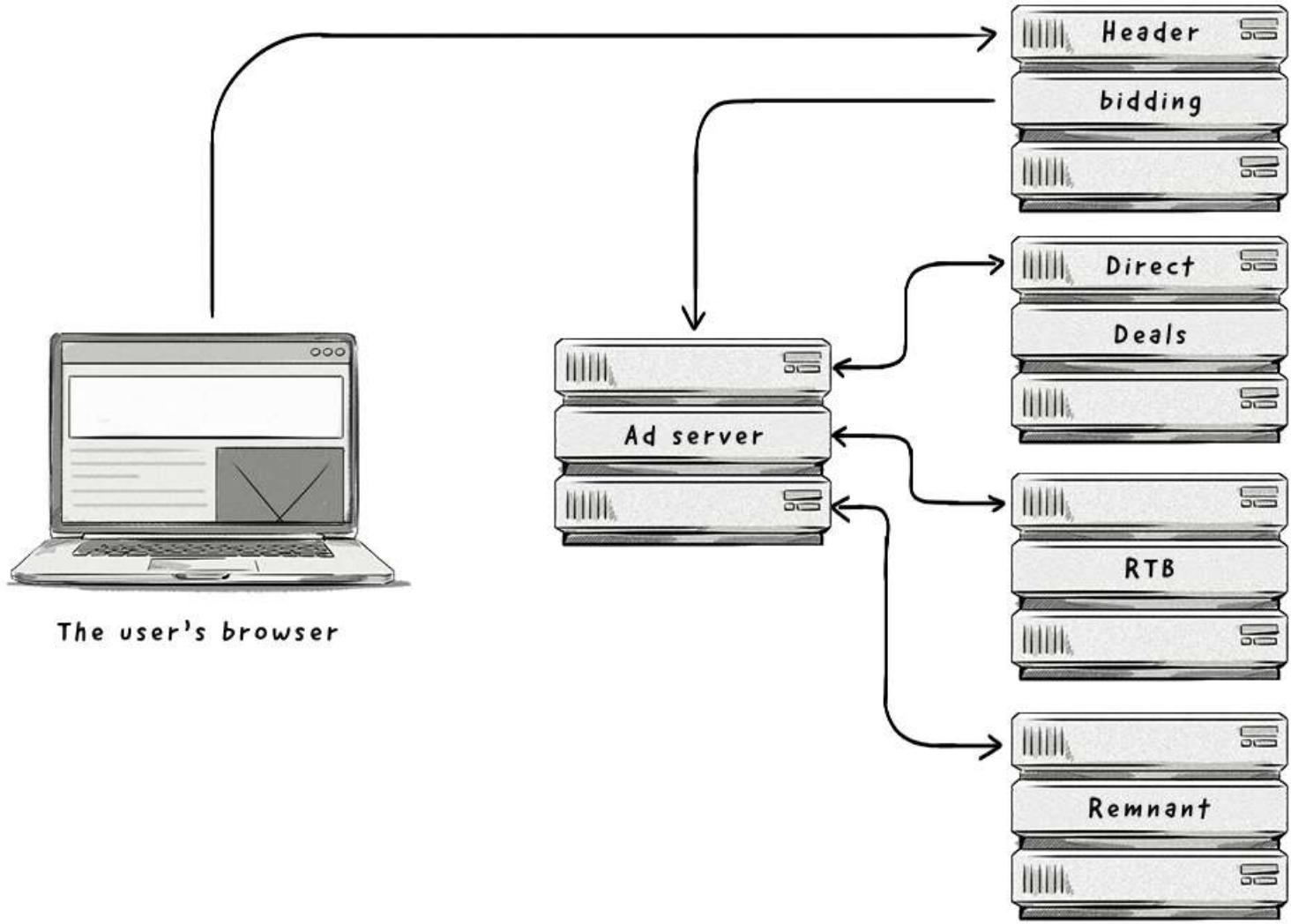
The drawback to this system is that some demand sources may be willing to pay a higher price for a given impression than their average historical yield.

For example, a remnant ad network third in the queue may have an average historical yield of \$2 CPM, but may be willing to pay \$5 CPM for a given impression if the user meets its targeting criteria.

This inability of waterfalls to accurately provide a real-time cost of available impressions was one of the reasons behind the rise of **header bidding**.

Header Bidding

Header bidding (aka **pre-bidding**, **advance bidding**, and **holistic yield management**) is a media-buying process that enables publishers to simultaneously collect bids from a number of demand sources (e.g. DSPs) before their ad server loads other tags, such as direct deals.



The bids are collected via a piece of JavaScript code located in a website's header section, hence the name header bidding.

Header bidding came about because of the inefficiencies of waterfalls and also because of Google's preferences towards its own ad products. Because many publishers use Google's ad server, formerly known as DoubleClick for Publishers (DFP), Google favored bids from Google Ad Exchange (AdX).

This resulted in demand from other AdTech platforms missing out on the chance to purchase the ad space, even if they wanted to pay a higher amount for it.

How Does Header Bidding Work?

To implement header bidding, publishers need to add a piece of JavaScript code (aka snippet or tag) in between the `<head></head>` tags on their website.

This JS code often comes in the form of a wrapper (aka container), which is typically provided by SSPs and ad exchanges.

Below is a [basic header-bidding example](#) from the open-source header-bidding wrapper, Prebid.js:

```
<html>

    <head>
        <link rel="icon" type="image/png" href="/favicon.png">
        <script async src="//www.googletagservices.com/tag/js/gpt.js"></script>
        <script async src="//acdn.adnxs.com/prebid/not-for-prod/1/prebid.js"></script>
        <script>
            var div_1_sizes = [
                [300, 250],
                [300, 600]
            ];
            var div_2_sizes = [
                [728, 90],
                [970, 250]
            ];
            var PREBID_TIMEOUT = 1000;
            var FAILSAFE_TIMEOUT = 3000;

            var adUnits = [
                {
                    code: '/19968336/header-bid-tag-0',
                    mediaTypes: {
                        banner: {
                            sizes: div_1_sizes
                        }
                    },
                    bids: [{
                        bidder: 'appnexus',
                        params: {
                            placementId: 13144370
                        }
                    }]
                },
                {
                    code: '/19968336/header-bid-tag-1',
                    mediaTypes: {
                        banner: {
                            sizes: div_2_sizes
                        }
                    },
                    bids: [{
                        bidder: 'appnexus',
                        params: {
                            placementId: 13144370
                        }
                    }]
                }
            ];
        </script>
    </head>
    <body>
        <div id="div-1" style="display:none;"></div>
        <div id="div-2" style="display:none;"></div>
    </body>
</html>
```

```

// ===== DO NOT EDIT BELOW THIS LINE ===== //
var googletag = googletag || {};
googletag.cmd = googletag.cmd || [];
googletag.cmd.push(function() {
    googletag.pubads().disableInitialLoad();
});

var pbjs = pbjs || {};
pbjs.que = pbjs.que || [];

pbjs.que.push(function() {
    pbjs.addAdUnits(adUnits);
    pbjs.requestBids({
        bidsBackHandler: initAdserver,
        timeout: PREBID_TIMEOUT
    });
});

function initAdserver() {
    if (pbjs.initAdserverSet) return;
    pbjs.initAdserverSet = true;
    googletag.cmd.push(function() {
        pbjs.que.push(function() {
            pbjs.setTargetingForGPTAsync();
            googletag.pubads().refresh();
        });
    });
}

// in case PBJS doesn't load
setTimeout(function() {
    initAdserver();
}, FAILSAFE_TIMEOUT);

googletag.cmd.push(function() {
    googletag.defineSlot('/19968336/header-bid-tag-0', div_1_sizes,
'div-1').addService(googletag.pubads());
    googletag.pubads().enableSingleRequest();
    googletag.enableServices();
});
googletag.cmd.push(function() {
    googletag.defineSlot('/19968336/header-bid-tag-1', div_2_sizes,
'div-2').addService(googletag.pubads());
    googletag.pubads().enableSingleRequest();
    googletag.enableServices();
});

</script>

</head>

<body>
<h2>Basic Prebid.js Example</h2>

```

```
<h5>Div-1</h5>
<div id='div-1'>
<script type='text/javascript'>
    googletag.cmd.push(function() {
        googletag.display('div-1');
    });

</script>
</div>

<br>

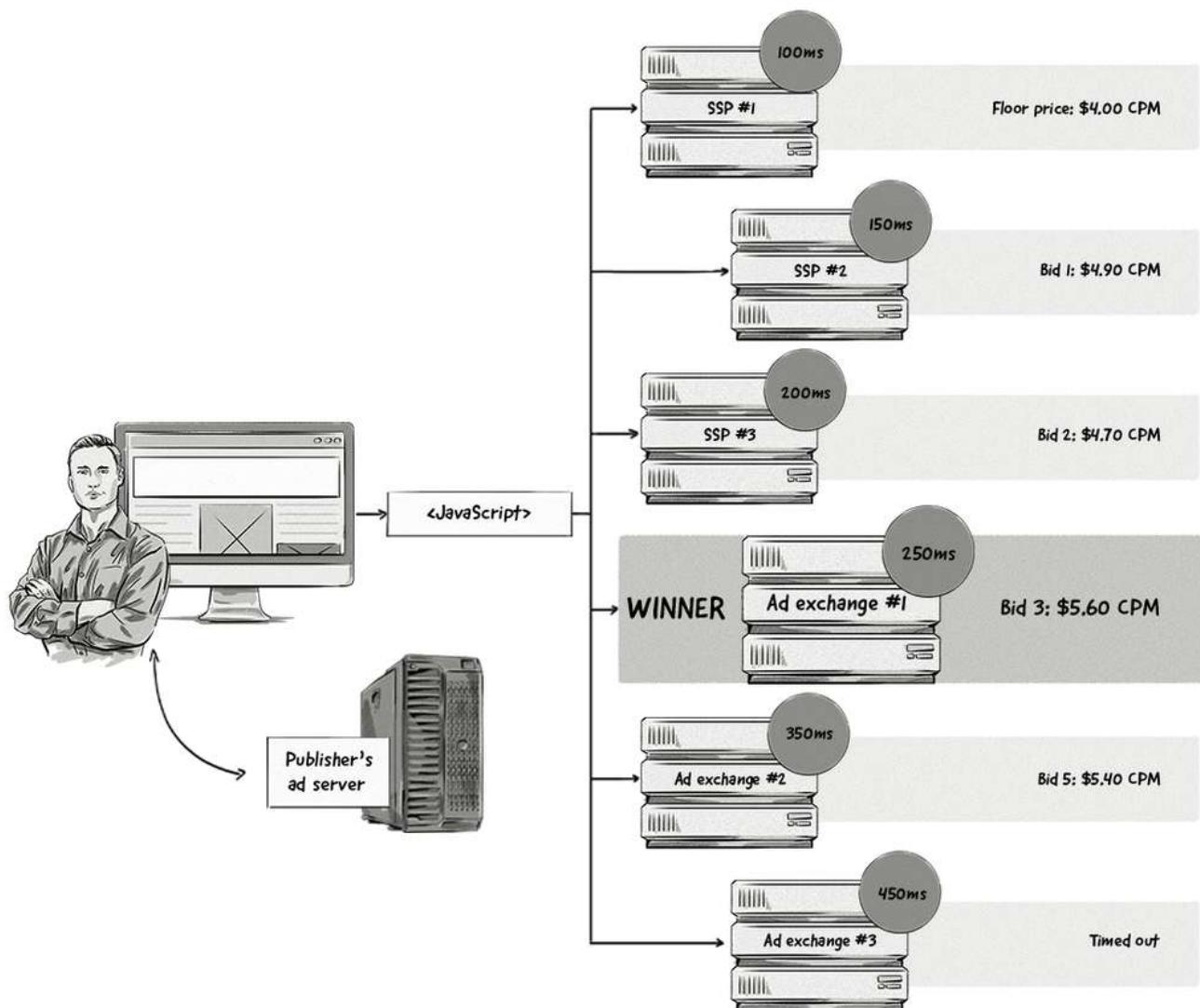
<h5>Div-2</h5>
<div id='div-2'>
<script type='text/javascript'>
    googletag.cmd.push(function() {
        googletag.display('div-2');
    });

</script>
</div>

</body>

</html>
```

Here's an overview of how the header-bidding process works:



Here's what is happening in the image above:

- A user opens their web browser and types in the publisher's URL (e.g. publisher.com).
- The browser starts loading the page.
- The header-bidding JavaScript code or wrapper located in the <head> tag executes and sends a request to the various AdTech platforms (SSPs and ad exchanges).
- The SSPs and ad exchanges send bid requests to multiple DSPs.
- The DSPs analyze the bids and return a bid response if the impression matches their campaigns.
- The highest bidder wins.
- The bid passes on to the publisher's ad server and competes with other campaigns, such as direct deals.
- If the DSP's bid is higher than the publisher's other campaigns, it is displayed to the user.

Just like other media-buying processes, latency is a big issue with header bidding.

If a DSP, SSP or ad exchange doesn't respond to the ad or bid request in time, they will be timed out and won't be able to submit a bid.

The timeout rates vary and are different on desktops, laptops, and mobile. On desktop and laptop computers, the timeout range is 400–800 milliseconds, and with mobile, it's 800–1,200 milliseconds.

Prebid.js – Making header bidding easier for publishers

Prebid.js is a 100% free and open-source JavaScript framework designed to make it easier for publishers to run pre-bid auctions and get access to more demand with minimal integration hassle. Available at prebid.org.

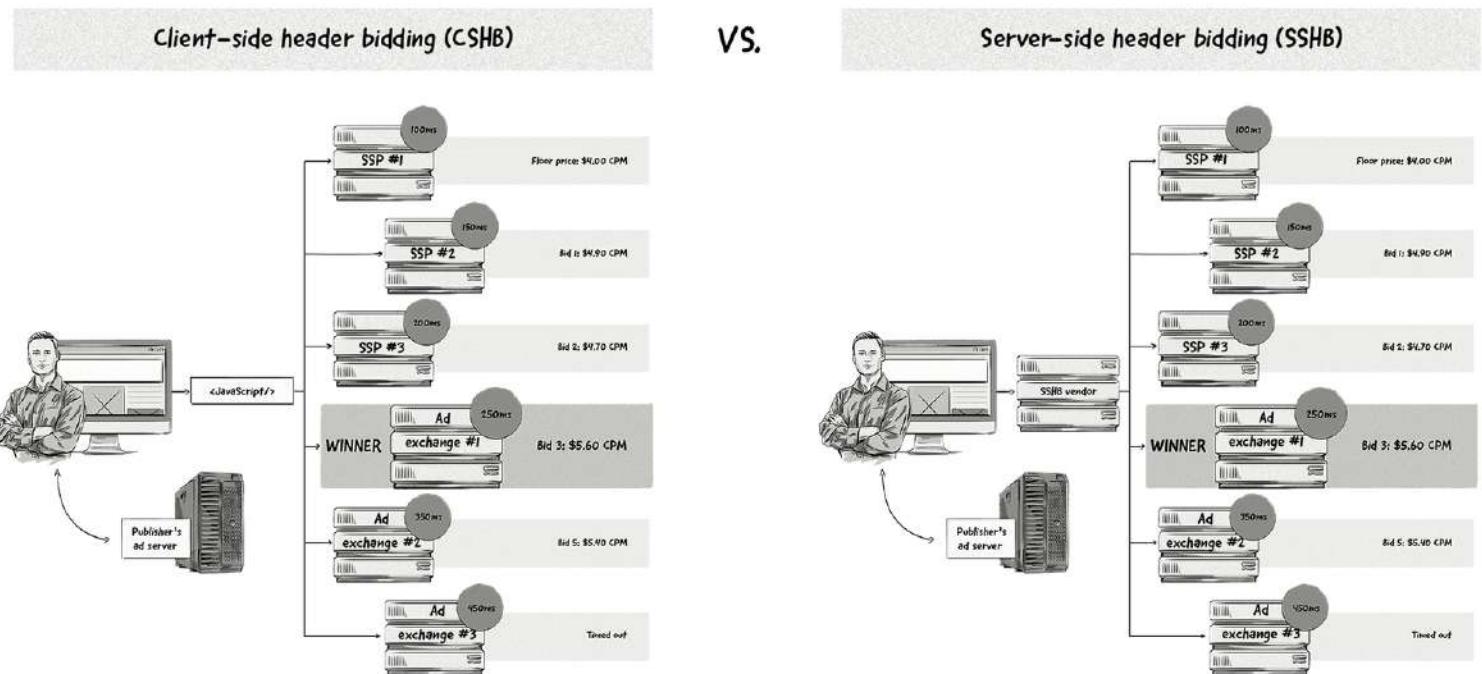
How to Implement Header Bidding: Client Side vs. Server Side

When it comes to implementing header bidding, there are two options: **client-side header bidding (CSHB)** and **server-side header bidding (SSHB)**.

Client-side header bidding collects bids directly from the web browser (i.e. the client), whereas server-side header bidding collects bids from a server.

With both CSHB and SSSH, the publisher still needs to add a wrapper or JS snippet to its website.

Here's a side-by-side comparison of how the client-side and server-side header-bidding implementations work:



Below are the main advantages and disadvantages of client-side and server-side header bidding.

Advantages of client-side header bidding:

- Cookie-matching rates are higher between AdTech platforms because the process happens in the browser.
- There's more control over header-bidding wrappers, meaning publishers can easily add and remove them.
- There's greater transparency into the demand sources and clearing prices.

Disadvantages of client-side header bidding:

- Because the header-bidding code is located on the page, it takes longer for the page to load, which provides a poor user experience.
- There may be some browser-compatibility issues, meaning the header-bidding code may not work properly on older browsers.
- Browsers can only make so many requests at one time, meaning the number of requests sent from a wrapper or tag will be limited to about a dozen or so.

Advantages of server-side header bidding:

- Page-load latency is significantly reduced because one call is made to a server, where all the bidding takes place on a server, instead of multiple calls being made from the browser.
- Server-side header bidding allows publishers to receive more bids from demand sources, as it doesn't have the same technical limitations as client-side.

Disadvantages of server-side header bidding:

- Because the process happens on a server, there's less control and transparency into things like clearing prices, demand sources and fees.
- Matching cookies is harder to do with server-side header bidding, which often leads to a drop in revenue for publishers because there's no addressability (i.e. advertisers don't know or can't identify the user on the website).

Waterfall vs. Header Bidding: Benefits and Drawbacks

The table below summarizes the main benefits and drawbacks of both the waterfall method and header bidding for publishers that want to increase fill rates and maximize yield.

Below we summarize the main benefits and drawbacks of both the waterfall method and header bidding for publishers that want to increase fill rates and maximize yield.

Benefits of the Waterfall

- Sells off remnant inventory that would otherwise be wasted.
- Compared to the header-bidding process, waterfalls are easier to implement and require less technical knowledge. In order to implement waterfalls, all the publisher needs to do is set up a tag on an ad network and in its ad server.

Benefits of Header Bidding

- Publishers can receive bids from buyers that may be more interested in their inventory (and willing to pay a higher price) than the buyers connected to the publisher's ad server.

- The chances of filling all types of available inventory, including both premium and remnant (unsold) inventory is higher because there are more buyers.
- Publishers are able to get greater insights into inventory value – e.g. if a publisher sets a floor price (the lowest price it is willing to sell inventory for) of \$1.50 CPM, but after utilizing header bidding finds that its inventory is being sold for an average of \$2.00 CPM, then it will get a clearer picture of how much its inventory is actually worth on the market.

Drawbacks of the Waterfall

- It can produce low yield, as the publisher's ad server chooses the demand sources based on the highest average yield, not the current market price of inventory, meaning the price given is the average CPM, not the true CPM.
- It often causes latency issues, as loading each tier takes time, and the more time passes, the less likely it is that the user will see the ad.
- Each demand source may fail to load the fallback or become timed out, resulting in lost revenue.
- Some demand sources require configuring the passbacks in their system, making it difficult for AdOps to reconfigure and manage.

Drawbacks of Header Bidding

- While header bidding may reduce the number of passbacks common in waterfall auctions, and thus improve page-load time, it has a few latency issues of its own (mainly caused by adding more scripts to a page). The latency issue is much less relevant with server-side header bidding.
- In order to work efficiently, client-side header bidding has to be backward-compatible with browsers and, in general, compatible with different browsers.
- If a publisher uses multiple header partners, it runs the risk of putting the same impression or inventory up for sale, duplicating its bid-processing efforts. This drawback relates to both client-side and server-side header bidding.
- Adding additional logic slows down the performance of the browsers and the website itself, which is not a big deal on modern hardware, but can be a problem on slightly older hardware and older smartphones.

Auction Dynamics: First- and Second-Price Auctions and Hard and Soft Floor Prices

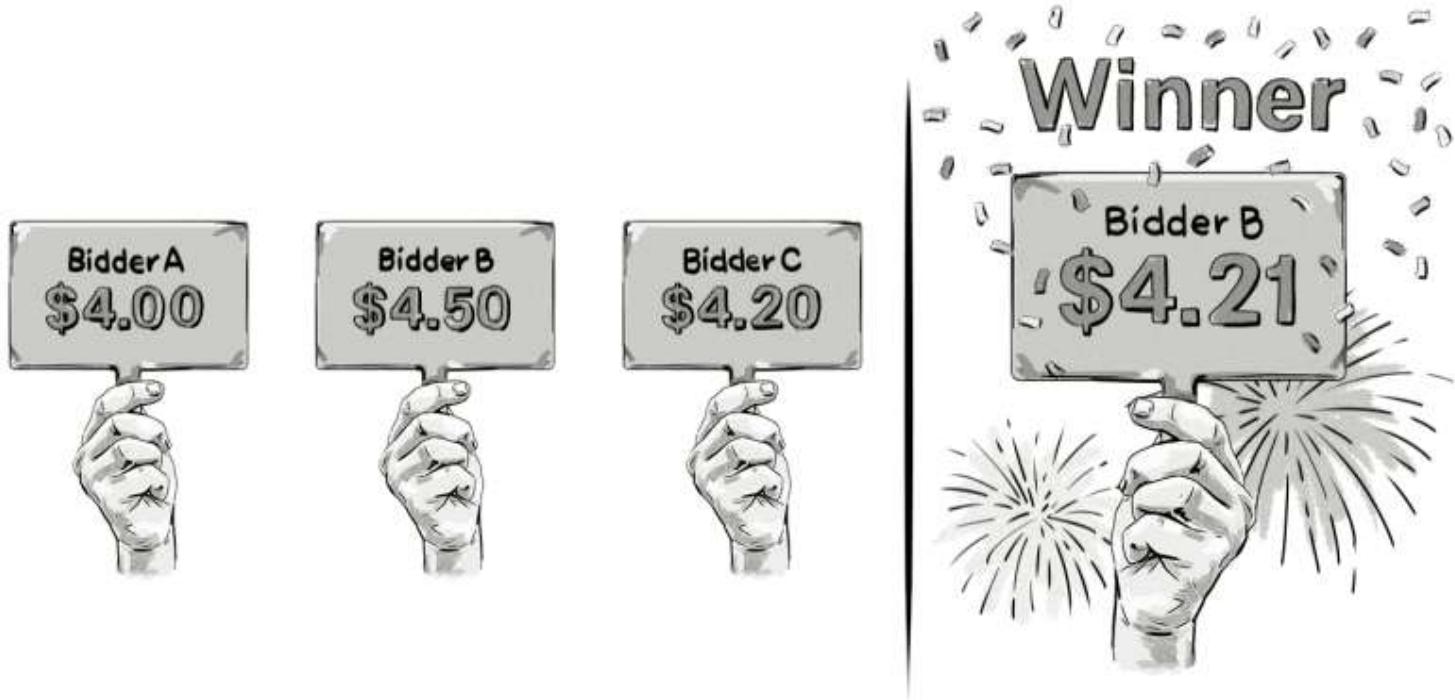
Auctions are an important part of many different types of transactions. They are used to buy and sell houses, works of art and products on ecommerce sites like eBay. They are also a key part of buying and selling online media via RTB transactions.

Since the beginning of real-time bidding towards the end of the 2000s, the main model used to buy and sell online media was the second-price auction.

Second-Price Auctions (2PA)

During second-price auctions (also known as Vickrey auctions), prospective buyers (advertisers) put forward their bids.

The winner is the highest bidder, but instead of paying the amount they bid, they pay the price put forward by the second-highest bidder plus \$0.01.



The price the buyer pays is known as the *clearing price*. The difference between the amount the advertiser bid and the clearing price is known as the reduction, or consumer surplus, which, in the example above, is \$0.29.

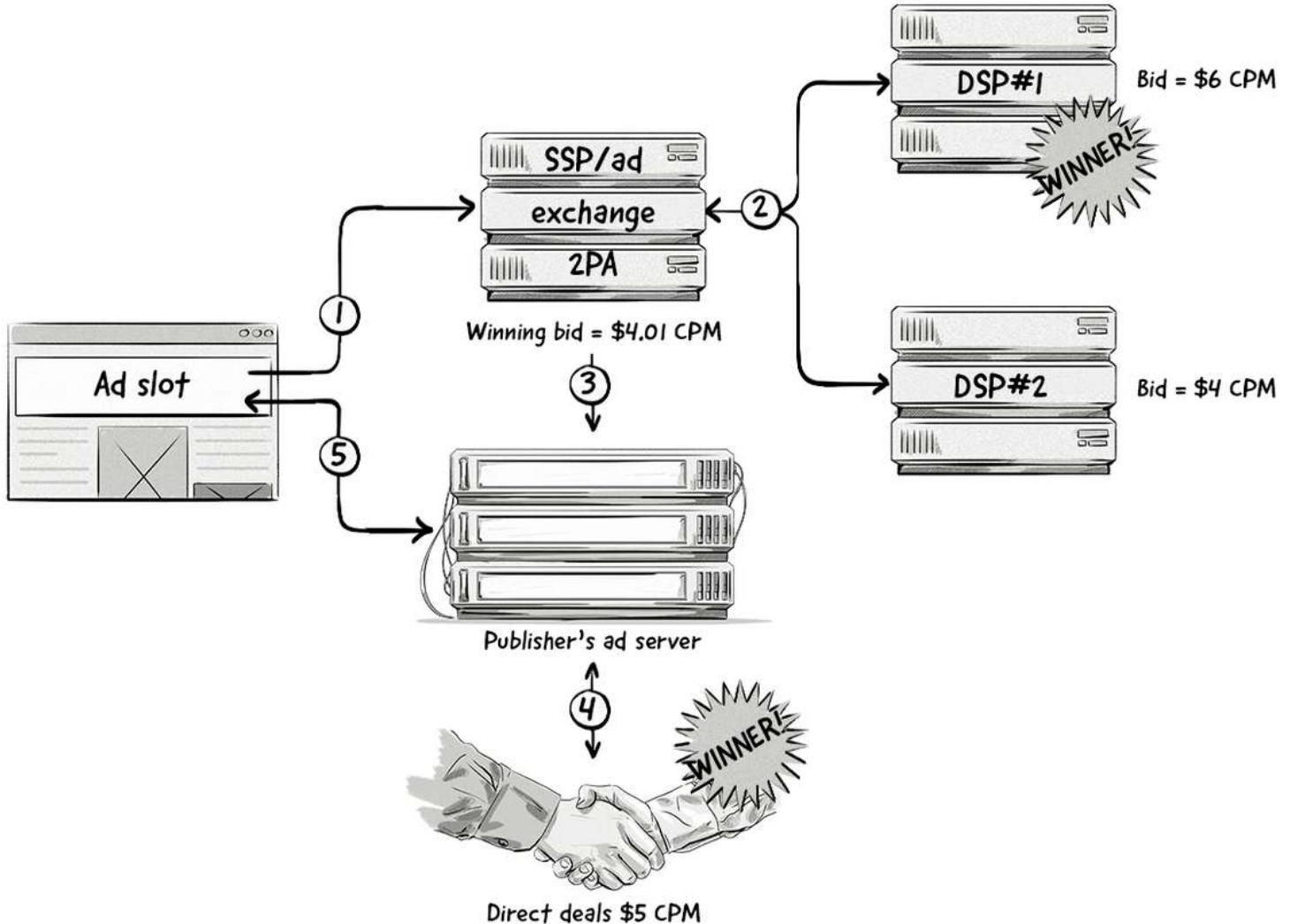
First-Price Auctions (1PA)

With first-price auctions, the highest bidder wins and pays the exact amount they bid. For example, if an advertiser bids \$2.50 CPM and they win the auction, the clearing price will be \$2.50 CPM.

The online advertising industry has used second-price auctions ever since the RTB model was introduced, but over the past couple of years (since 2017/2018), many ad exchanges and SSPs have started moving to first-price auctions.

The main reasons for this are to counter the impact of header bidding and make auctions more transparent and fair for advertisers and publishers.

Despite the advantages of header bidding, many advertisers were losing out to direct deals, even though their initial bid was higher. This meant that publishers were missing out on higher CPMs.

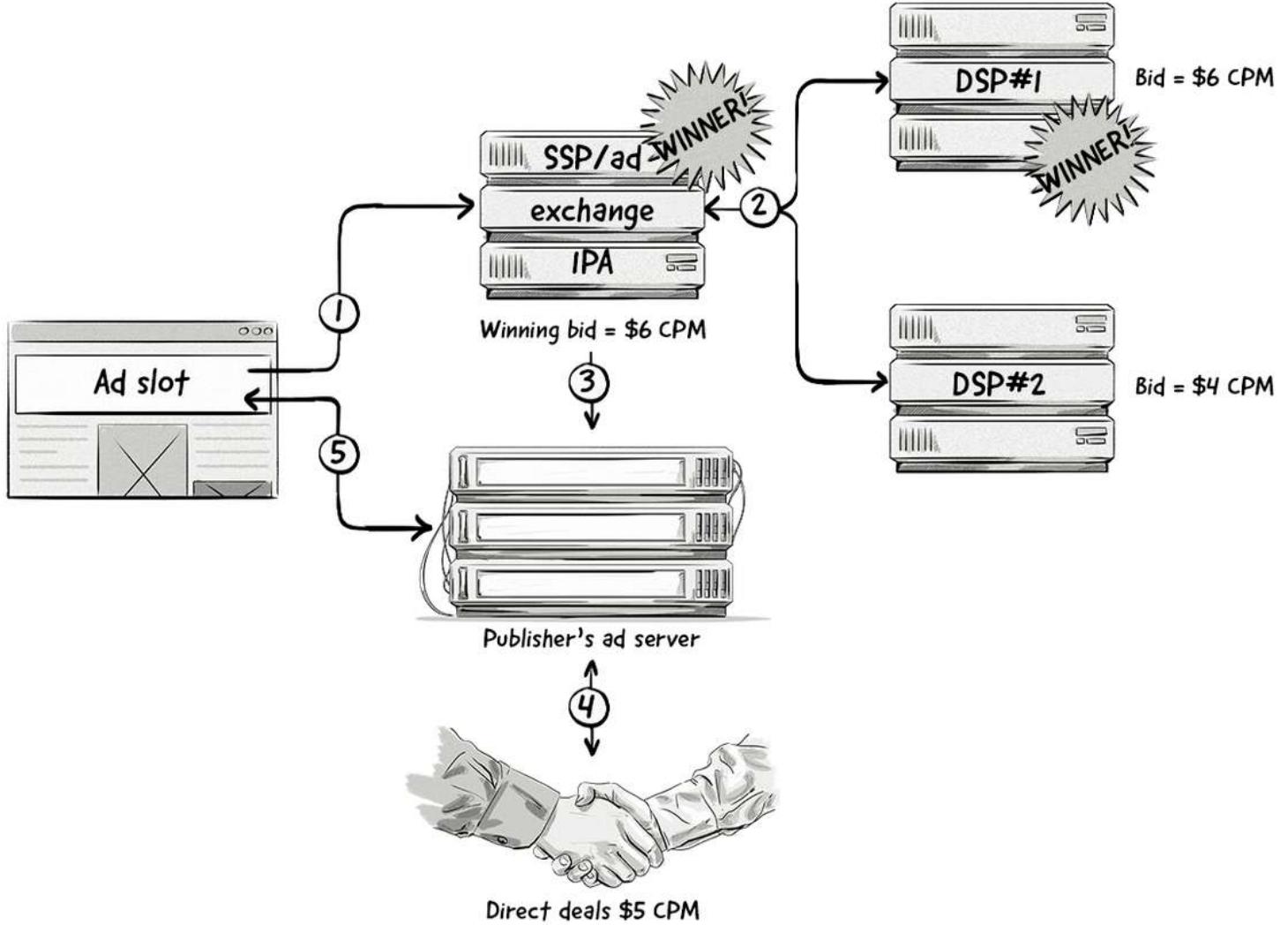


Step-by-step explanation:

- The publisher's web page loads and a header-bidding request is sent to an SSP/ad exchange.
- The SSP/ad exchange sends a bid request to DSPs. Each DSP returns a bid response with its respective bid. Because the SSP/ad exchange conducted a second-price auction, the winning DSP pays \$0.01 more than the second-highest bid (DSP #2), which works out to be \$4.01.
- The SSP/ad exchange passes DSP #1's winning bid to the publisher's ad server. This bid will now compete with a publisher's direct deals.
- In this case, the direct deal is higher than the bid from DSP #1 (\$4.01), so the direct deal wins.
- The ad from the direct deal is sent to the web page and displayed to the visitor.

As the diagram above illustrates, the advertiser (represented by DSP #1) missed out on showing its ad to the visitor even though it was willing to pay more than the direct deal. This is a common pitfall of the second-price auction model with header bidding.

Let's look at how this same situation is improved with first-price auctions.



Now, because a first-price auction was held between the SSP/ad exchange and the two DSPs, the winning bid from the header-bidding auction is \$6.00 CPM, which is exactly what DSP #1 bid. Because it is higher than the direct deal, its ad is shown to the visitor.

Bid Shading

While the move from second-price auctions to first-price auctions allows advertisers to win more impressions, they are now having to pay a higher price.

If advertisers were bidding \$5.00 CPM but winning most impressions for \$3.01 on a second-price auction, they would now be paying \$5.00 CPM on a first-price auction. As you can imagine, this has a big impact on media budgets and spend.

What's more, second-price auctions give advertisers a pretty good idea of how much the impressions are worth, allowing them to change their bids accordingly. With first-price auctions, there's really no easy way for advertisers to know this.

To help advertisers optimize their bids during first-price auctions and get them closer to the real cost of the bid, AdTech companies introduced a feature known as **bid shading**.

Bid shading is essentially an algorithm that aims to tell advertisers how much they should bid on first-price auctions. It does this by analyzing historical bid data, such as how much the impression was selling for, the ad position and at what price bids are lost.

At the moment, bid shading is offered by supply-side platforms and some demand-side platforms. The reason for this is because most DSPs haven't updated their tech to handle first-price auctions.

Although bid shading helps advertisers save money, it's not a very transparent practice.

It's quite easy for an AdTech company to tell an advertiser that they should be bidding \$3.00 CPM when the actual impression would sell for \$2.00 CPM and then pocket the difference. The only way an advertiser would know the true cost of an impression would be to obtain data from the SSP, which is not something that happens in programmatic advertising.

While most AdTech vendors offer bid shading as a free feature, there's talk that many vendors will start charging for this, which has angered advertisers, as they feel that optimizing their bids should be something their tech partners offer as standard.

Bid shading also leaves publishers with less ad revenue. Instead of an advertiser bidding \$5.00 CPM and winning, if they use bid shading and win the bid at \$3.00 CPM, that's money the publisher has missed out on.

Floor Prices

The contract between an AdTech vendor and publisher will typically specify a minimum CPM price that the ad network is to offer its advertisers.

This guaranteed CPM price is also called a **floor price** and is designed to avoid the situation where the AdTech vendor may discount the publisher's inventory, which would devalue it in the eyes of advertisers.

There are two types of floor prices: **hard and soft**.

Hard price floor

A hard price floor represents the minimum price the publisher will accept for the impressions.

Any bids below this minimum price are simply ignored, meaning publishers will not accept any bids below the hard price floor.

Soft price floor

Because bidders may not necessarily know what the hard floor is, many publishers set a soft floor price to "catch" any bids that fall slightly below the publisher's asking price and that otherwise would get rejected.

No winner

Rejected bids



Hard price floor = \$4.25

Bids taking part in 1st price auction

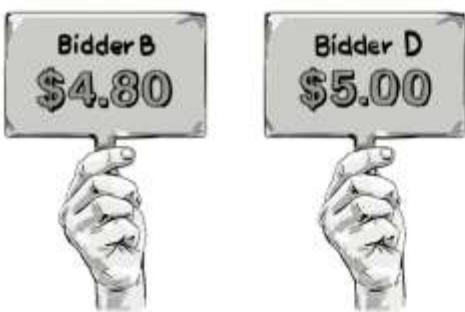


Winner



Soft price floor = \$4.75

Bids taking part in 2nd price auction



Winner



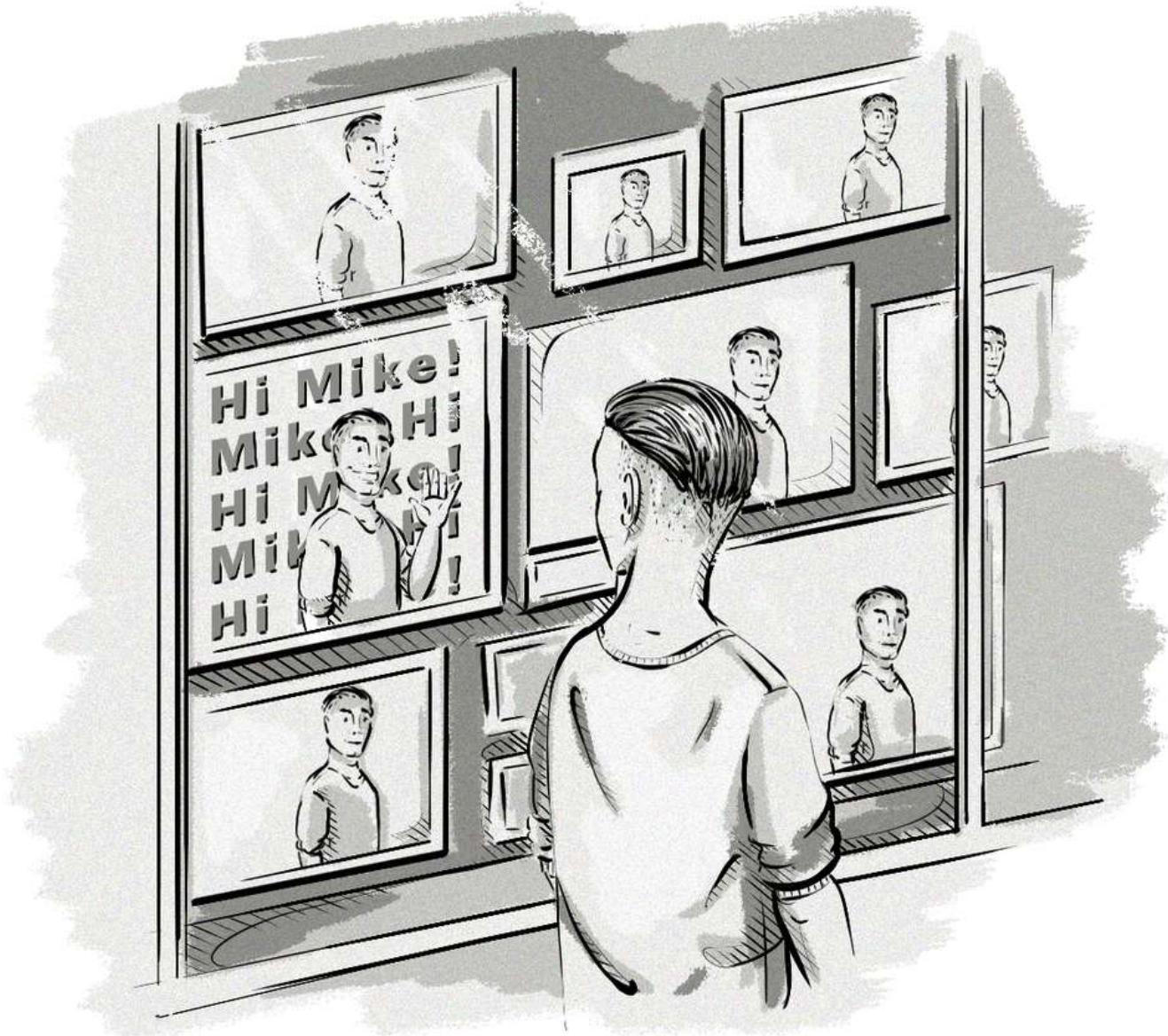
As we can see in the image above, the hard price floor automatically ignores all bids under \$4.25.

Any bids between the hard and soft floor take part in a first-price auction. If there are bids above the soft price floor, they will take part in a second-price auction.

Chapter Summary

- There are many different ways advertisers can buy online media from publishers, such as:
 - **Direct deals:** Deals made directly between a publisher and advertisers.
 - **Programmatic direct:** An advertiser and publisher agree on the inventory and the CPM, and the rest of the process is handled programmatically (i.e. via the use of AdTech platforms).
 - **Real-time bidding (RTB):** Real-time auctions where advertisers bid on individual impressions offered by publishers via DSPs, ad exchanges and SSPs.
 - **Private marketplace (PMP):** An invite-only version of RTB whereby publisher's allow certain advertisers to bid on their inventory before they offer it in an open RTB auction.
- Waterfalling is a process used by a publisher to sell all remnant inventory whereby the publisher's ad server calls the demand sources one after another.
- Header bidding is a process that allows publishers to collect bids from multiple demand sources before their ad server is called, which increases their chances of securing higher CPMs.
- There are two main auction types in RTB:
 - Second-price auctions, where the winning bid pays the second-highest price plus \$0.01.
 - First-price auctions, where the winning bid pays the amount they bid.
- Floor prices allow publishers to set a minimum CPM that they are willing to accept for their inventory.

10. User Identification



Earlier in the book, we looked at how AdTech platforms use various targeting methods to display ads to the right audience, but how do they know whether a person on a given website or mobile app is part of their target audience?

The answer: via user identification methods.

Why Do We Need to Identify Users?

- To power behavioral targeting and content personalization.
- To run retargeting/remarketing campaigns.
- To measure the reach of campaigns.

- To track conversions.
- To attribute sales and conversions to impressions and clicks.
- To apply frequency capping.

Different User-Identification Methods

The process of identifying users depends on the type of device they are using (e.g. a smartphone or laptop) and whether they are using a web browser or mobile app.

For example, a user visiting web pages in a web browser, either on a mobile device or computer, would be identified by browser-based identification methods.

A user playing a mobile-app game on a smartphone or tablet would be identified by a mobile identifier.

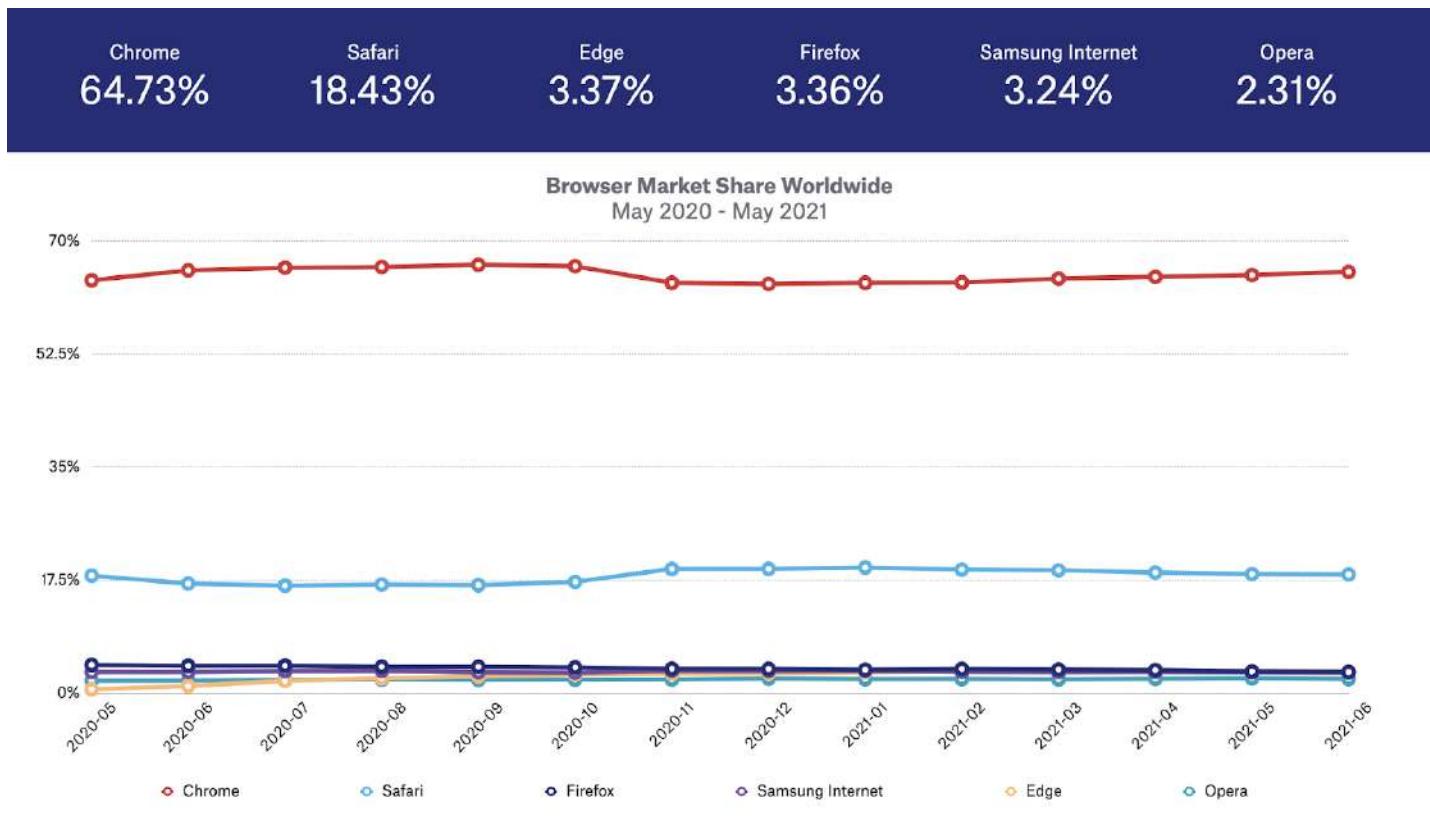
Let's take a closer look at these identification methods.

Web Browsers

Web browsers have been around since the beginning of the Internet and allow users to access websites on desktops, laptops and mobile devices.

According to statcounter, the most popular [web browsers globally](#) based on market share are:

- Google Chrome (64%)
- Apple Safari (18%)
- Mozilla Firefox (3%)



Source: [Statcounter](#), 2021.

The above illustrates the global market share of the most popular web browsers, but this changes when adding in variables such as country and device.

For example, in Germany, [Firefox has 13% market share](#) compared to a 5% global market share.

Similarly, Apple's Safari web browser is the most popular web browser on iOS-powered devices like iPhones and iPads, and Chrome is the most popular web browser on Android devices

The table above illustrates the global market share of the most popular web browsers, but this changes when adding in variables such as country and device.

For example, in Germany, Firefox has 14% market share compared to a 4% global market share.

Similarly, Apple's Safari web browser is the most popular web browser on iOS-powered devices like iPhones and iPads, and Chrome is the most popular web browser on Android devices.

The main browser-based user-identification methods are **cookies**, **device fingerprints** and **HTML local storage**.

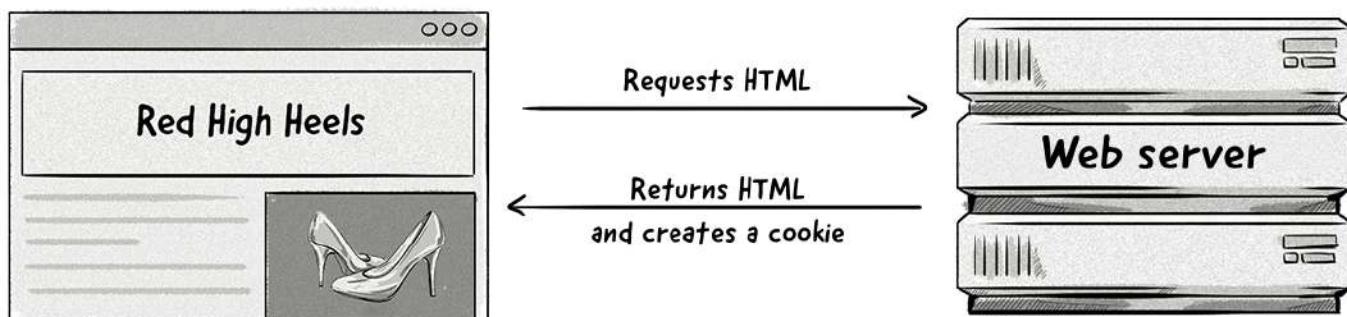
Cookies

Cookies (aka web cookies, HTML cookies and browser cookies) are small files that are placed on a user's device by a web server when accessing websites.

Web cookies were created by Lou Montulli in 1994 as a way to remember stateful information in an otherwise stateless environment.

What that means is that the [HTTP protocol](#), which is the main protocol for communication between a web browser and a web server, is a stateless process; it can't store any data or information, it can only receive requests and respond to them.

Cookies are used to help web browsers store data and information when communicating with web servers via the HTTP protocol.



When a user returns to a website they've previously visited, cookies will help the website remember certain things, such as what content the user viewed and which pages they accessed.

Some of the main uses of cookies include:

- **Website setup:** Cookies can help web browsers remember user preferences, such as language and currency.
- **Sign in:** To keep users logged in to their accounts, a unique session ID is stored in a cookie so the user won't have to log in to their account each time they open their browser.
- **eCommerce:** Cookies used by eCommerce stores help web browsers remember which products users viewed, added to the shopping cart and purchased.
- **Analytics:** Cookies are used to store a user identifier that collects data about the user's interaction with the website under one profile and session, such as which pages they visited, what areas they clicked on and if they completed any goals (e.g. downloaded an ebook).
- **Behavioral targeting and advertising:** AdTech platforms use cookies to identify users and show relevant ads to them based on their previous behavior, such as which websites and pages they've visited. Cookies also help advertisers and publishers know which ads they've viewed and clicked on.

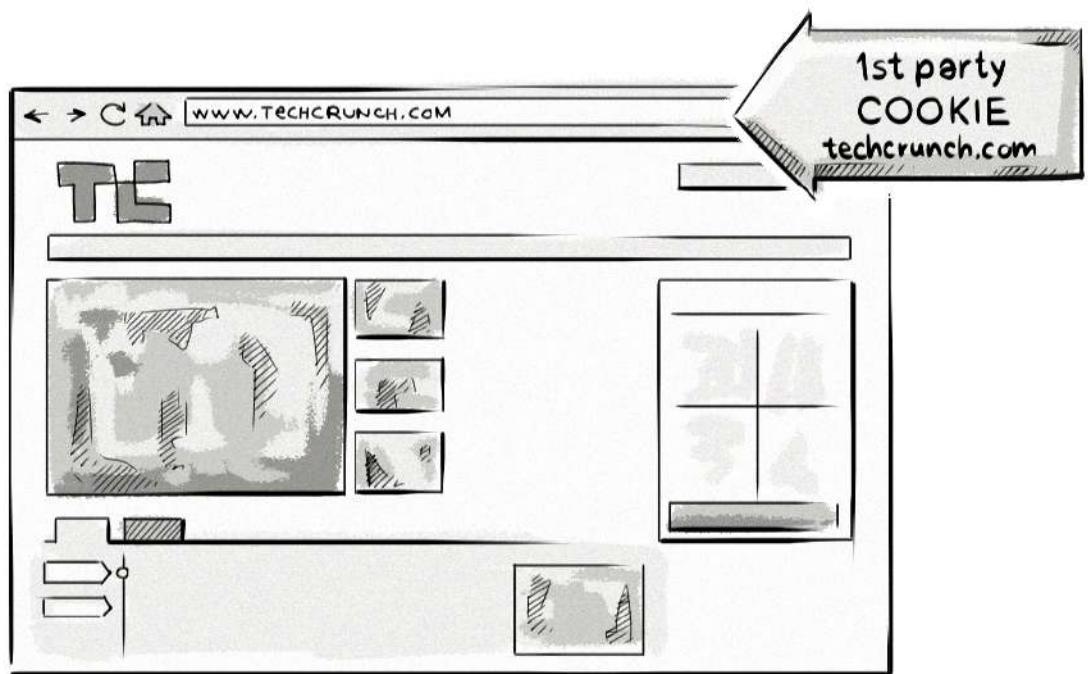
Cookies have been the most common method for identifying users on web browsers since the early days of the Internet, however, the rise of privacy laws, such as the European Union's General Data Protection Regulation (GDPR) and privacy features in browsers (e.g. Safari's Intelligent Tracking Prevention) are restricting the creation and access to cookies (*more on that below*).

Different Types of Cookies

For the most part, all cookies are the same. However, there are two main types of cookies: **first-party** and **third-party cookies**.

The difference has to do with the relationship between the website and the server that created them.

First-party cookies are created by the domain (website) a user visits directly. For example, if you visit techcrunch.com, then it will create some first-party cookies and save them to your device.



First-party cookies are created by the domain the user is visiting.

First-party cookies are typically used to deliver a good user experience by remembering specific information and user preferences.

For example, first-party cookies help websites remember the language a user has set and which products they've added to a shopping cart.

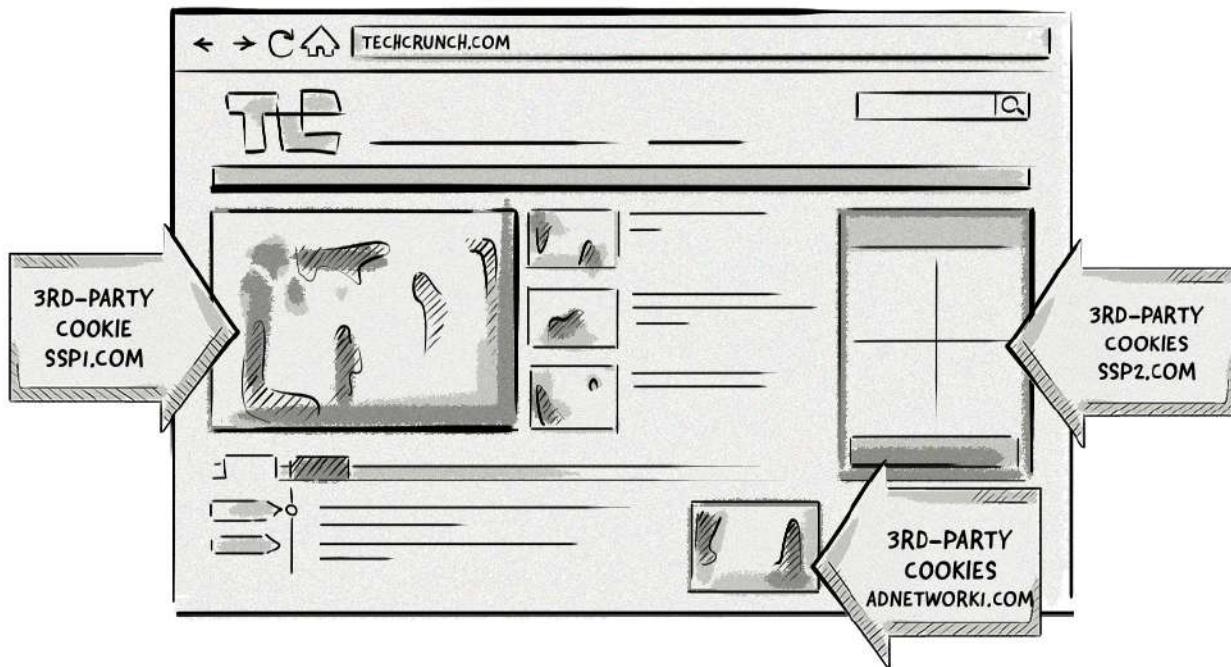
Also, first-party cookies can allow users to stay logged in to websites and accounts, meaning they don't have to log in each time they visit their favorite websites.

Although they can be used for online advertising, they are limited in their ability to identify users across different domains. This means that a first-party cookie created by ssp1.com on techcrunch.com can't be read by ssp1.com on different websites.

In order to overcome this limitation, AdTech companies use third-party cookies and cookie syncing to identify users across different websites (*more on that below*).

Third-party cookies, also referred to as tracking cookies and third-party trackers, are created by domains other than the one the user is on.

For example, if you visit techcrunch.com and it loads a piece of JavaScript from an AdTech platform (e.g. ssp1.com), a first-party cookie would be created for techcrunch.com and a third-party cookie would be created for ssp1.com.



Because ssp1.com is not the domain the user is visiting, it is classed as a third-party cookie.

All other cookies created by domains other than techcrunch.com would also be classed as third-party cookies.

Third-party cookies have long been the backbone of online advertising, allowing AdTech companies to identify users as they move around the web, run targeted ad campaigns based on a user's behavior, and attribute impressions, visits, clicks and conversions.

However, third-party cookies are becoming less effective due to privacy laws like the GDPR, privacy features in browsers like Safari's Intelligent Tracking Prevention and Firefox's Enhanced Tracking Prevention, and browser plugins like AdBlock Plus and Ghostery.

How First-Party and Third-Party Cookies Are Created

The image below illustrates how first-party and third-party cookies are created by web browsers.

Server-side method



With the server-side method, cookies are created by the Set-Cookie HTTP response header.

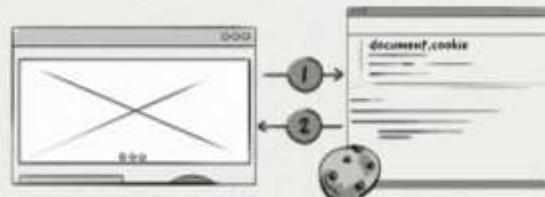
- 1 The web browser loads a resource, such as an image, that sends a HTTP request to a server (e.g. AdTech platform) to retrieve it.
- 2 The server sends back a HTTP response with the Set-Cookie header.

With every subsequent request to the web server, the browser will send information about the cookie to the server.

Here's an example of a HTTP response with Set-Cookie header:

```
HTTP/2.0 200 OK
Content-type: text/html
Set-Cookie: id=hyt6298gt6sdfl7
```

Client-side method



With the client-side method, cookies are created via programming languages, e.g. JavaScript.

- 1 The web browser loads a piece of JavaScript from a server (e.g. AdTech platform).
- 2 The JavaScript creates a cookie in the user's device.
The JavaScript tag would also be used to read the cookies that were set previously.

Here's an example of document.cookie

```
document.cookie = "sspl=hyt6298gt6sdfl7";
```

With the first method, AdTech platforms can either create cookies via the ad creative when it's retrieved from their server or via a 1x1 transparent image. The goal of the 1x1 transparent image is simply to get the browser to send a request to the AdTech platform's browser so it can create a cookie when it returns the image.

Comparison of First-Party and Third-Party Cookies

	First-Party Cookies	Third-Party Cookies
Setting and Reading the Cookie	<ul style="list-style-type: none"> Can be set and read by the publisher's web server or JavaScript loaded on the website. 	<ul style="list-style-type: none"> Can be set on different websites via JavaScript or by loading resources from servers (e.g. 1x1 transparent pixels). Once a third-party cookie is set to a user's device, it is read when the user visits other websites that also load the AdTech platform's JavaScript or request a resource.
Availability	<ul style="list-style-type: none"> It can only be read by the domain that the user is visiting. 	<ul style="list-style-type: none"> It's available on any website that loads the AdTech platform's JavaScript or 1x1 transparent pixel.
Browser Support	<ul style="list-style-type: none"> Supported by all browsers. 	<ul style="list-style-type: none"> Supported by all browsers.
Blocking and Deletion	<ul style="list-style-type: none"> Relatively small deletion rates. The exception is Safari's Intelligent Tracking Prevention feature that either deletes first-party cookies after 24 hours or seven days. <i>More on that at the end of this chapter.</i> 	<ul style="list-style-type: none"> An increasingly high deletion and blocking rate. Third-party cookies are blocked by browsers such as Tor, Safari and Firefox, and also blocked by ad-blocking browser plugins like AdBlock Plus and Ghostery.

Remember flash cookies?

Flash cookies act similarly to HTTP cookies but are created via the Adobe Flash plugin, which is used to power things like videos and mobile apps.

About a decade ago, the use of Flash cookies raised a number of privacy concerns due to the lack of control users had with deletion. Flash cookies were stored in a separate folder on devices and could only be managed via the Adobe Flash settings, meaning that when a user deleted their HTTP cookies, their Flash cookies remained intact.

This led to Adobe and popular web browsers making changes to how Flash cookies were handled. Since then, Flash cookies are treated the same as HTTP cookies, so if a user deletes their HTTP cookies, Flash cookies would also be deleted.

For this reason, and because many videos and games are played via HTML5 nowadays, the use and availability is much lower than in the past, therefore they aren't used for online advertising anymore.

Cookie Syncing

Because cookies created by one domain can't be read by another, this makes it hard for AdTech platforms to identify the same user on a given web page.

For instance, if a user visits example.com, the cookie that the SSP creates will be different than the one a DSP creates.

To help AdTech platforms identify the same user on different websites, a process known as cookie syncing was developed.

Cookie syncing is the process of mapping one user ID (stored in a cookie) from one technology platform to another (e.g. from a DMP to a DSP). The eventual goal of syncing cookie IDs is to share data about the user between different platforms, which allows them to better target audiences with online advertisements. The two platforms would have a formal agreement between one another and would need to set up partner IDs on their platforms and add cookie-syncing pixels in their codes.

The cookie-syncing process is carried out by a number of different platforms in the ecosystem, including data-management platforms (DMPs), demand-side platforms (DSPs), ad networks, ad exchanges, supply-side platforms (SSPs) and many more.

How Does Cookie Syncing Work?

There are two main parts to the cookie-syncing process:

- Mapping of cookie IDs
- Sharing of user data contained in the cookies

Mapping Cookie IDs

Each time a user visits a website that contains a cookie-syncing pixel or other advertising-platform tag, the browser sends a request to a technology platform – for example, a DSP.

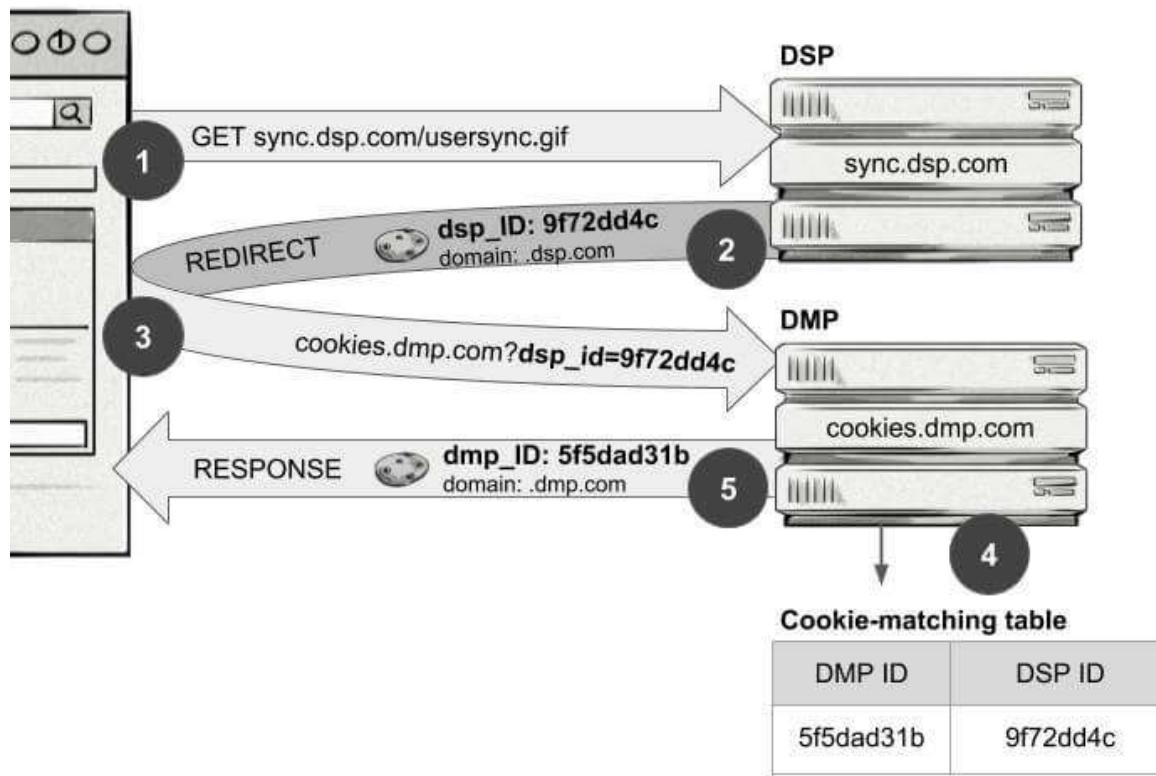
The DSP creates a unique ID for that user, if one doesn't exist already, and stores that ID in a cookie. The DSP then redirects (http redirect) the request to the cookie-syncing endpoint URL that has been supplied by a different advertising platform – for example, a DMP – and passes the user ID as a URL parameter.

The DMP's server reads the user ID created by the DSP from the parameter in the URL and reads the cookie in its own domain to see if it already has an ID for this particular user. If it doesn't, the server creates a user ID of its own, then stores the information about its own ID and the DSP's ID in a cookie-matching table.

The DMP can pass its own identifier back to the DSP so that the sync is bidirectional. It does this by doing a pixel redirect back to the DSP and passes its own ID as a parameter.

Now, both the DSP and DMP have each other's user IDs in each other's databases.

The image below illustrates how the cookie-syncing process looks.



Sharing Data Between Two Platforms

Once the cookie IDs have been synced between two AdTech platforms, they can share or request data contained in the cookies by referencing each other's user IDs.

Typically, this process is done via a server-to-server integration with the data being transferred in large batch files. Unlike the cookie-matching part that happens in real-time, sharing the data between platforms happens at a specified time – for example, once a day.

It's important to note that cookie syncing is only performed in web browsers (desktop or mobile) across all types of online advertising, including display, native and video ads.

The reason for this is because unlike native mobile apps that use the device's advertising ID (e.g. IDFA and AID) as a way to identify users, web browsers don't emit a consistent user identifier. Cookies from one domain can't be accessed by a platform operating under a different domain, so the only way to identify a user across different websites is by using their cookie ID.

Problems With Cookie Syncing

Although cookie syncing allows AdTech companies to identify users across the web, it has a couple of inherent problems:

- The more cookie syncs a web page needs to perform, the longer it takes the page to load, which can result in a bad user experience.
- Cookie-match rates vary among platforms, with the average rate sitting between 40-60%.
- Cookie churn, caused by third-party cookies being blocked by default or regularly deleted by users, means the effectiveness and accuracy of cookie syncing decreases.

Cookie Respawning

Cookie respawning is a process whereby a cookie reappears, or respawns, after it has been deleted.

It does this by using backed-up data stored in additional files on a user's device and then respawning the cookie later when a user accesses the same website again.

The process looks like this:

1. A user accesses a website.
2. The website creates a cookie.
3. The cookie tags the user's browser with a unique identifier that is not easy to delete.
4. The user leaves the website and deletes their cookies.
5. The user accesses the website again and the new cookie recognizes the identifier in the browser and respawns the original cookie.

There are two main ways a cookie can be respawned:

Flash cookies: Companies use the Adobe Flash Player browser plugin to store information about the user on their computer and to respawn cookies. As mentioned above, flash cookies are rarely used these days.

HTML5: HTML5 local storage and cache cookies use entity tags (ETags) to respawn HTML cookies by recognizing the persistent identification element (PIE) created by JavaScript and Flash.

Device Fingerprinting

Device fingerprinting is a technical process that aims to identify and track online users based on the characteristics of their devices. It works by gathering bits of information to create an identifier, which is then used to identify individuals across different websites.

While many different users may own the same device, each one will be configured slightly differently according to the user's individual preferences and requirements. Data about these configuration changes can be aggregated to create a recognizable "device fingerprint."

Information used to create a device fingerprint can include:

- Browser version
- Operating system
- Language
- Items installed (plugins, fonts, etc.)
- Location and time-zone settings
- Browser settings

Here's an example of the HTTP header attributes that are used to create a device fingerprint:

HTTP headers attributes		
Attribute	Similarity ratio ⓘ	Value
User agent ⓘ	0.04%	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:70.0) Gecko/20100101 Firefox/70.0
Accept ⓘ	52.93%	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content encoding ⓘ	63.61%	gzip, deflate, br
Content language ⓘ	27.80%	en-US,en;q=0.5
Upgrade Insecure Requests ⓘ	20.45%	1
Do Not Track ⓘ	9.57%	1
Referer ⓘ	11.80%	https://amiunique.org/

Showing 1 to 7 of 7 entries

Check out what your device fingerprint looks like at <https://amiunique.org> or <https://panopticlick.eff.org/>

The image above illustrates how unique certain attributes are to the user's device, as represented by the similarity ratio.

For example, the user agent has a similarity ratio of 0.04%, meaning it is very unique to this user.

The more unique the attribute is, the more easily it can be used to identify a user.

Why Do Companies Use Device Fingerprinting?

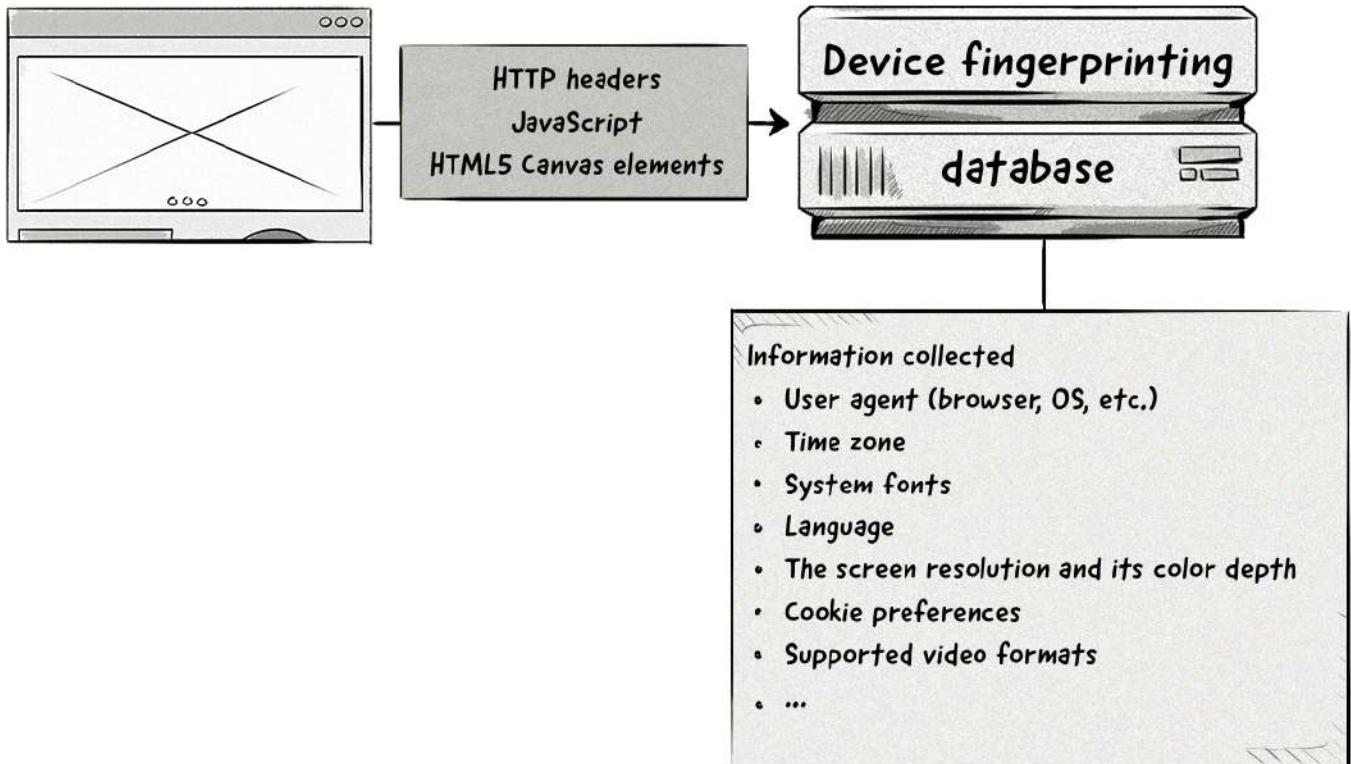
Device fingerprinting emerged to address a number of challenges that AdTech and analytics companies faced around the availability and reliability of cookies.

Over the past decade, online users have regularly deleted and blocked cookies via ad-blocking plugins and browser settings to protect their online privacy.

This has made it harder for AdTech and analytics companies to identify and track users across the web.

Although device fingerprinting isn't as accurate as cookies, it can be used as a backup when cookies are blocked or deleted, as well as in combination with cookies to help increase the chances of identifying a particular user.

How Does Device Fingerprinting Work?



Creating a device fingerprint requires collecting data and information about a user's device, which is typically collected via:

- The user agent and accept headers
- JavaScript
- Flash plugin (if installed)
- HTML5 canvas elements

What is canvas fingerprinting?

Canvas fingerprinting is similar to device fingerprinting, but only uses the HTML5 canvas element to identify a browser.

Companies use a piece of JavaScript to instruct the user's web browser to draw a picture via the canvas. Each browser will draw a slightly different image, meaning the image is unique (or highly unique) to the device. This allows companies to identify and track users across the web.

This information is then combined and a unique hash is created and assigned to that device.

Unlike cookies that are stored on a user's device (client-side), device fingerprints are stored in a database (server-side) due to the amount of information they collect.

HTML5 Local Storage

HTML5 local storage is a newer method for collecting and storing data about users.

There are two variants of local storage:

localStorage: Stores data with no expiration date.

sessionStorage: Only stores data for the session – i.e. data is deleted when the user closes the browser tab.

Compared to cookies, HTML5 local storage provides the following benefits:

- **More storage:** HTML5 local storage can store up to 5MB of data, compared to 4KB (4096 bytes) for cookies.
- **More availability:** Most browsers don't delete HTML5 local-storage data and it isn't typically blocked by ad-blocking plugins or browser settings.
- **No web-server calls:** To create cookies, a request needs to be sent from a web page to a web server and then back again. HTML5 local storage is created via JavaScript and doesn't require any calls to servers.

The main downside from an AdTech perspective is that it is domain- and protocol-specific, meaning users can't be identified across different domains.

ETags

An entity tag (ETag) is an HTTP response header used to improve the efficiency of cache and save bandwidth.

It does this by assigning an identifier to content (e.g. images) on a web page.

When a web page loads, the browser sends off a request to various web servers to retrieve the contents.

If a URL has an ETag set for a given resource (e.g. an image), the web server will compare the incoming ETag with its own ETag. If the two match, it means the image hasn't changed. The web server will then tell the browser that the image in the cache is still up to date and can be displayed on the web page.

AdTech companies can identify users by comparing the ETags sent from a user's browser with their records.

To achieve this, a publisher would need to install an AdTech's HTML code on their website, typically a 1×1 transparent image (aka pixel).

When the page loads, the code will load and send a request containing an ETag to the AdTech vendor's server.

If the ETag coming from the publisher matches the ETag in the AdTech vendor's server, they would be able to identify the browser.

Because it's a standard HTTP request, the AdTech vendor could also collect information about the user, such as their operating system, browser type, language, location and the URL they are visiting. This information can be used to create audiences and later for ad targeting.

Information created via ETags will be deleted if a user clears or deletes their browser's cache.

Evercookies

An evercookie is a cookie that is saved to various storage locations in a user's browser and device. It was created by the privacy and security researcher, Sammy Kamkar.

Companies can create evercookies via a JavaScript API, which saves data in various locations. If the user deletes data from one location, such as HTTP cookies, the JavaScript API will recognize that this data has been removed and simply respawn the cookie from one of the other storage locations.

The current list of storage locations includes:

- Standard HTTP cookies
- Local shared objects (Flash cookies)
- Silverlight Isolated Storage
- Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 canvas tag to read pixels (cookies) back out
- Storing cookies in web history
- Storing cookies in HTTP ETags
- Storing cookies in web cache
- Window.name caching
- Internet Explorer userData storage
- HTML5 session web storage
- HTML5 local web storage
- HTML5 global storage
- HTML5 web SQL database via SQLite
- HTML5 IndexedDB
- Java JNLP PersistenceService
- Java CVE-2013-0422 exploit (applet sandbox escaping)

Because evercookies are much harder to delete than regular HTTP cookies, they raise a number of privacy concerns.

The table below outlines the advantages and disadvantages of the various methods used to identify users via web browsers.

Method	Advantages	Disadvantages
First-Party Cookies	<ul style="list-style-type: none">• Supported by all browsers.• Relatively small deletion rates.	<ul style="list-style-type: none">• Cannot identify users across different domains.• Safari restricts first-party cookies created by known trackers (e.g. AdTech companies).

Third-Party Cookies	<ul style="list-style-type: none"> • Supported by all browsers. • Can identify users across different domains. 	<p>Third-party cookies are often blocked when a user does one or more of the following:</p> <ul style="list-style-type: none"> • Browses the web in private or incognito mode. • Uses Safari or Firefox as their web browser. • Changes the cookie and tracking settings in their browsers. • Uses Tor. • Installs ad blockers or similar add-ons.
Device Fingerprints	<ul style="list-style-type: none"> • Can identify users across different domains. • Are stored on a server, rather than on a device, meaning they can't be deleted by the user. 	<ul style="list-style-type: none"> • Become inaccurate if a user changes their browser's settings or uses a different browser. • Cannot be reset or deleted by users, leading to privacy issues. • Corporate environments where many computers have the same configuration can produce duplicates.
HTML5 Local Storage	<ul style="list-style-type: none"> • Very small deletion rates. • Can store more data than cookies. • Data doesn't need to be appended to HTML requests. 	<ul style="list-style-type: none"> • Cannot be used to identify users across different domains.
ETags	<ul style="list-style-type: none"> • Can be created as part of an HTTP request and doesn't require additional JavaScript. • Can identify users across different domains. 	<ul style="list-style-type: none"> • All ETags are removed if a user clears their browser's cache.
Evercookies	<ul style="list-style-type: none"> • Combines the advantage of the above data storage and user identification techniques (and many more). • Highly persistent and hard for users to delete and block. 	<ul style="list-style-type: none"> • Raises a number of privacy concerns, as there is no easy way for users to block or delete evercookies.

How Different Web Browsers Handle Cookies, Device Fingerprints and Local Storage

					
First-Party Cookies	Accepted by default. Can be deleted by the user.	Accepted by default. Can be blocked and deleted by the user.	Accepted by default. Most first-party cookies created by AdTech companies (classified trackers) via link decoration expire in 24 hours.	Accepted by default.	Accepted by default.
Third-Party Cookies	Currently accepted by default, but will be stop being supported by 2022.	Blocks third-party trackers (aka cookies) by default.	Blocks third-party trackers (aka cookies) by default.	Some known third-party trackers are blocked by default.	Accepted by default. Users can block third-party cookies by changing the browser's privacy settings.
Device Fingerprints	Currently, Chrome doesn't block device fingerprinting, but will likely block fingerprints from Chrome 80, which is planned to launch in February 2020.	Can be created with the Standard privacy setting, but are blocked if a user changes this setting to Strict.	Safari sends a simplified system profile, which makes it harder to create unique device fingerprints.	IE doesn't block device fingerprinting.	Opera 64 and newer versions of the browser block trackers including some fingerprinting scripts.
HTML5 Local Storage	Available on version 4 and above without restrictions.	Available on version 3.5 and above without restrictions.	All data stored in local storage will be deleted after seven days.	Available on version 8 and above without restrictions.	Available on version 10.4 and above without restrictions.
ETags	Available without restrictions.	Available without restrictions.	Available without restrictions.	Available without restrictions.	Available without restrictions.
Evercookies	Can be created via the above methods. Users can remove evercookies by deleting all browsing and storage data.	Can be created via the above methods.	Can be created via the above methods. Users can remove evercookies by deleting all browsing and storage data.	Can be created via the above methods.	Can be created via the above methods.

In private and incognito modes, all cookies are deleted when the session ends – i.e. when the user closes the browser.

How to See Which Cookies Are Saved During a Web Session

You can see which first-party and third-party cookies, as well as data in other storage locations, are created during a session in your web browser by doing the following:

Chrome: Right-click on the page ⇒ Inspect ⇒ Application

Firefox: Right-click on the page ⇒ Inspect Element ⇒ Memory

Safari: Right-click on the page ⇒ Inspect Element ⇒ Storage

Internet Explorer: Press F12 ⇒ Console tab ⇒ Type “sessionStorage” or “localStorage” in the console

Edge: Follow the above instructions for Chrome (it looks the same because both browsers are based on Chromium)

Opera: Follow the above instructions for Chrome (it looks the same because both browsers are based on Chromium)

The screenshot shows a browser window displaying The New York Times homepage. At the top, there is a dark banner with the text "NAVY THE TEAM WORKS" and a "APPLY NOW" button. Below the banner, the main navigation menu includes links for ENGLISH, ESPAÑOL, and 中文. On the far right, there is a "Log In" button. The main content area features the iconic New York Times masthead. At the bottom of the page, there is a navigation bar with links for World, U.S., Politics, N.Y., Business, Opinion, Tech, Science, Health, Sports, Arts, Books, Style, Food, Travel, Magazine, T Magazine, Real Estate, and Video. A date stamp indicates it is Tuesday, November 12, 2019. To the left of the main content, the developer tools' "Elements" tab is active, showing the DOM structure. Below the Elements tab, the "Cookies" tab is selected, displaying a list of cookies. The table has columns for Name, Value, Domain, Path, Expires /..., Size, HttpOnly, Secure, and SameSite. Many cookies are listed under the domain ".nytimes.com", such as "IP_JAR", "CONSENT", "IDE", "NID", "S", "UID", "UIID", "cfduid", "gads", "cb", "cb_ls", "cb_svref", "chartbeat2", "gcl_au", "ad-id", "ad-privacy", "h2b_cig_opt", "bkdc", "phx", "bku", "data", "data-a", "data-o", "data-r", and "edu_cig_opt". Other cookies are listed under domains like ".google.com", ".doubleclick.net", ".scorecardresearch.com", ".iteratehosting.com", ".nytimes.com", ".amazon.com", ".media.net", and ".bluekai.com". The "SameSite" column shows values like "None" and "None" (with a checkmark).

Name	Value	Domain	Path	Expires /...	Size	HttpOnly	Secure	SameSite
IP_JAR	2019-11-12-10	.google.c...	/	2019-12-...	19			None
CONSENT	WP28022c	.google.c...	/	2038-01-...	16			
IDE	AHWtUk6EwcxrGhmqlp4BLSpV4ppMEYNRReq1SRpXE...	.doublecl...	/	2021-11-...	67	✓		
NID	191-vRtb4FwbujELUOxDok5l8PFTb70uqCrYRHEKfCDQs9i...	.google.c...	/	2020-05-...	178	✓		
S	billing-ui-v3=xAR9xDKW1uyLqIGH8a/gwbElpa3n1v:billing...	.scorecar...	/	2021-10-...	36			
UID	1DD10494a1001249beee4g1573197682	.scorecar...	/	2021-10-...	14			
UIID	1573197682	.iterateh...	/	2020-11-...	51	✓		
_cfduid	dc29f2109a7651138e0f66fd4aa7d2561573553714	.nytimes...	/	2021-11-...	75			
_gads	ID=e0a537401e50b6ca:T=1573553702:S=ALNI_Mbu0WFw...	.nytimes...	/	2020-12-...	20			
_cb	BAWEv2DPNPpxf2W2e	.www.nyti...	/	2020-12-...	7			
_cb_ls	1	.www.nyti...	/	2020-12-...	40			
_cb_svref	https%3A%2F%2Fwww.google.com%2F	.www.nyti...	/	2019-11-...	74			
_chartbeat2	.1573553710546.1573553710546.1BmyT1sBLz_n6BeOps...	.www.nyti...	/	2020-12-...	32			
_gcl_au	1.1.1736367632.1573553703	.nytimes...	/	2020-07-...	28	✓		
ad-id	A0KlqOEockB4mPJwd3zY6Kc	.amazon...	/	2025-01-...	11	✓		
ad-privacy	0	.amazon...	/					
h2b_cig_opt	%7B%22isCorpUser%22:false%7D	.nytimes...	/	2019-11-...	45			
bkdc	phx	.bluekai...	/	2020-05-...	7	✓		None
bku	5LD99Ybs0ktjUuTo	.bluekai...	/	2020-05-...	19	✓		None
data	[[REDACTED]]	.media.net	/	2020-11-...	62			
data-a	1339249325733955082~-1	.media.net	/	2020-02-...	28			
data-o	ca9d7ccf-6ada-0928-2b12-a9b98502e230~-1	.media.net	/	2020-11-...	45			
data-r	K2VP8VuJ-1Y-CYV0~-1	.media.net	/	2020-05-...	25			
edu_cig_opt	%7B%22isEduUser%22:false%7D	.nytimes...	/	2019-11-...	38			

The screenshot above shows which cookies are created in Chrome when a user visits The New York Times website. Under the Cookies tab on the left, we can see that a bunch of first-party cookies were created under the nytimes.com domain. All the cookies under that domain are third-party cookies.

Mobile Devices

In the section above, we explained how users can be identified when browsing the Internet via a web browser on a desktop or laptop.

Now we will look at the ways in which advertisers can identify and track users when using a web browser and apps on mobile devices, such as smartphones and tablets.

Here's an overview of the user-identification methods on mobile devices:

Mobile Environment	User Identification	Details
Mobile Web Browsers	First-party cookies	Accepted by all major browsers.
	Third-party cookies	Blocked by most of the popular web browsers by default, except Chrome.
In-App	Cookies	Some mobile apps can create cookies via webview, but these cookies are app-specific and can't be shared with other apps.
	Google Advertising ID	More persistent than cookies and can be used to identify users (devices) across different apps. Can be reset by users, but can't be blocked or deleted completely.
	Apple's Identifier for Advertising (IDFA)	More persistent than cookies and can be used to identify users (devices) across different apps. Can be reset by users but can't be blocked or deleted completely.
	Open Device Identification Number (ODIN)	In 2012, ODIN was created by eight AdTech companies to solve the identity issue on mobile devices. This solution was made redundant when advertising IDs were introduced.

Mobile Web Browsers

Web browsers on mobile devices typically handle cookies in the same way as on desktop or laptops.

Here's an overview of how web browsers handle cookies on mobile devices.

					
First-Party Cookies	Accepted by default.	Accepted by default. Some first-party cookies are set to expire in 7 days.	Accepted by default.	Accepted by default.	Accepted by default.
Third-Party Cookies	Accepted by default, but can be blocked by changing the settings. Third-party cookies will be blocked by default from 2023.	Third-party cookies and data are limited by default.	Known trackers are blocked by default, meaning third-party cookies from AdTech companies will be blocked.	Accepted by default.	Accepted by default.

Mobile Apps (In-App)

Identifying users in mobile apps (aka in-app) can consist of the following methods:

Cookies

To display online content inside web apps, some app developers use a piece of technology called webview.

Webview can create cookies and store them inside a secure location on the device, which is known as a sandbox or sandboxed environment.

The main issue for AdTech is that these cookies are app-specific, meaning they can't be shared across different apps, therefore AdTech companies can't identify the same user across different apps even though they are using the same device.

Advertising IDs

Mobile devices include an advertising ID:

- Google's Android ID (AID)
- Apple's ID for Advertising (IDFA)
- Microsoft's Advertising ID (aka Advertising Identifier)

These IDs are more persistent than web cookies, and even though users can't disable or remove these IDs like they can with cookies, they can easily reset them.

The exception to this is Apple's IDFA, which is only available to app developers and AdTech companies if users opt in via the AppTrackingTransparency (ATT) framework. This framework applies to apps running on iOS 14.5 iPadOS 14.5, and tvOS 14.5 and above.

Read more about Apple's ATT framework in chapter 14. User Privacy in Digital Advertising.

How Are Advertising IDs Used for Identification in Mobile Apps?

Advertising IDs are passed from mobile apps to AdTech platforms. Below is an example of a real-time bidding (RTB) bid response showing a mobile ID in the *ifa* field.

```
"device": {  
  
    "dnt": 0,  
  
    "ua": "Mozilla/5.0 (iPhone; CPU iPhone OS 6_1 like Mac OS X)  
AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A334 Safari/7534.48.3",  
    "ip": "123.145.167.189",  
    "ifa": "AA000DFE74168477C70D291f574D344790E0BB11",  
    "carrier": "VERIZON",  
    "language": "en",  
    "make": "Apple", "model": "iPhone",  
    "os": "iOS", "osv": "6.1",  
    "js": 1,  
    "connectiontype": 3,  
    "devicetype": 1,  
    "geo": {  
  
        "lat": 35.012345, "lon": -115.12345,  
        "country": "USA",  
        "metro": "803",  
        "region": "CA", "city": "Los Angeles", "zip": "90049"  
  
    }  
}
```

Did you know?

Apart from advertising IDs, there are even more persistent IDs in mobile devices – Universal Device Identifier (UDID) and Media Access Control (MAC) Address.

These IDs are associated with the hardware of mobile devices and can't be disabled or reset by users. There was a time when Apple and Google allowed access to these IDs, but due to privacy reasons (i.e. they can't be disabled or reset), they stopped providing access to them in 2012 and 2013 respectively.

Open Device Identification Number (ODIN)

[Back in 2012](#), eight mobile-advertising companies came together to develop an alternative to the Universal Device Identifier (UDID) and Media Access Control (MAC) Address.

The solution was called the Open Device Identification Number (ODIN).

However, this solution has since been replaced by advertising IDs provided by Google and Apple.

User Profile Matching

As we've just covered, identifying users via one method can be incredibly difficult and inaccurate.

The problem is exacerbated when users use more than one device, which is often the case nowadays.

Currently, there is no method that allows AdTech vendors to identify users as they move from one device to another.

The reason for this is because the traditional ways of identifying and tracking users with cookies in web browsers wasn't designed for the multi-device world.

There are, however, two ways you can identify and track the same user as they move across different devices with reasonable accuracy: **deterministic matching** and **probabilistic matching**.

Deterministic and Probabilistic Matching

Deterministic and probabilistic matching are processes used to identify users across different devices.

Companies will often use both deterministic and probabilistic matching together to increase match rates.

What Is Deterministic Matching?

Deterministic matching involves creating a profile of users consisting of different pieces of data about them.

These profiles are then used to identify users on different devices by looking for a common identifier.

Common identifiers can include:

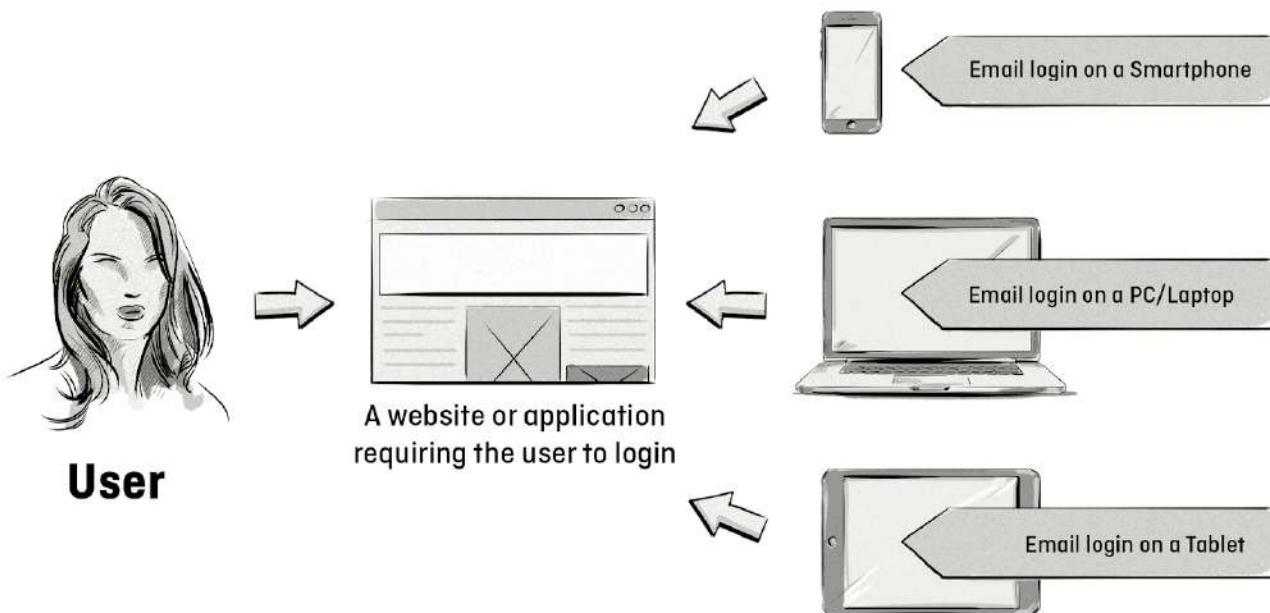
- Email address
- First and last name (if uncommon)
- Address
- Date of birth
- Phone numbers

It's important to note that this information would be hashed when it's collected to remove personally identifiable information.

How Does Deterministic Matching Work?

The most common way to deterministically match users in online advertising and marketing is by using an email address as the common identifier, as this is unique to the user and is often available in different data sets.

Companies like Facebook, Google, Twitter and LinkedIn are able to deterministically match users with ease and accuracy because they require users to create accounts and sign in using an email address to access their applications and sites on different devices.



How deterministic matching works.

The main advantage of deterministic matching is accuracy. It's much more accurate than probabilistic matching; most deterministic matching rates are around 80-90%.

The main drawback, however, is that it lacks scale, as most companies don't collect this type of data and email addresses aren't typically used for buying and selling online advertising.

To address the issue of scale, publishers are requiring users to create an account or subscribe using their email address to access certain content.

The two main ways they can do this are:

By way of encouragement: Publishers can encourage visitors to provide an email address in exchange for more access and content.

By way of force: Publishers can gate their content and restrict access to it unless users subscribe or create an account.

These tactics would work well with large publishers like news sites, as they typically have an engaged audience that regularly visits their sites compared to small- and medium-sized publishers, as not everyone will want to create an account just to read a few blog posts.

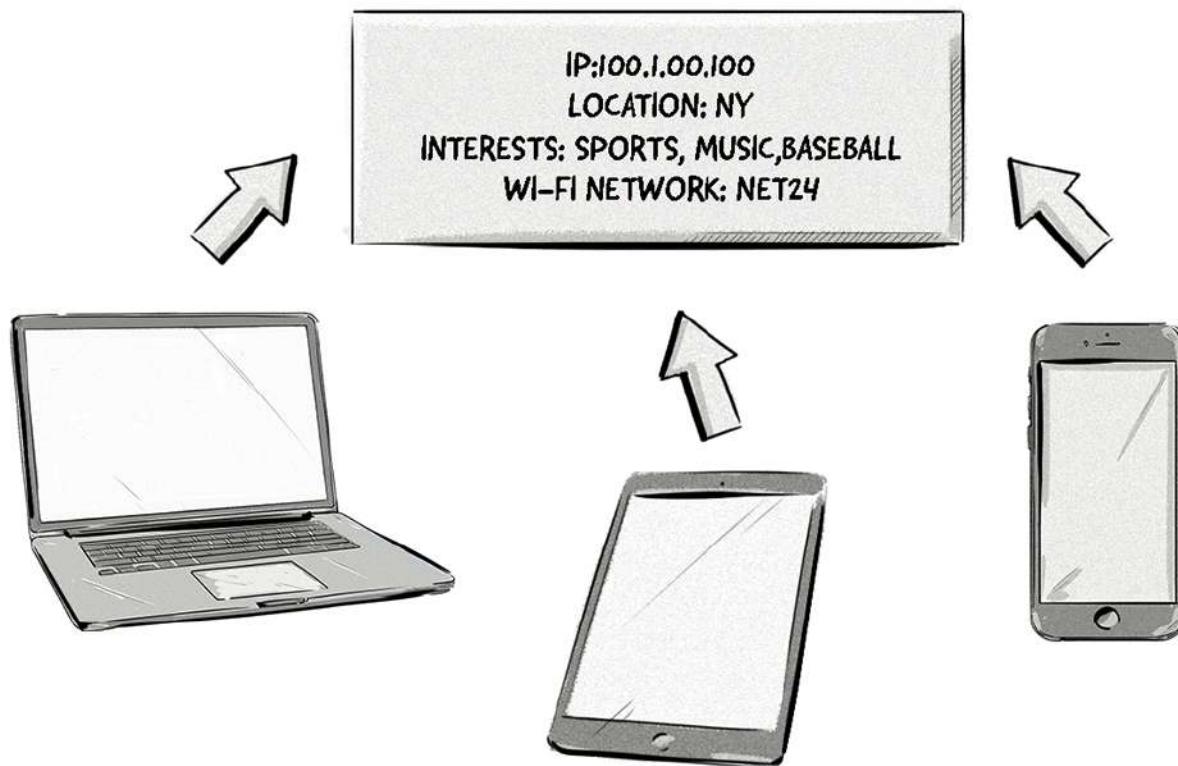
What Is Probabilistic Matching?

Unlike deterministic matching that uses a common identifier, such as an email, to match users to devices and applications, probabilistic matching uses various pieces of data, algorithms, and statistical modeling to make a match.

The type of data used for probabilistic matching includes:

- IP address
- Location
- Interests, behavior, and browsing history
- Wi-fi networks

The image below illustrates how one user operating all three devices can be probabilistically matched to all of them based on their IP address, location, interests and Wi-fi network.



How probabilistic matching works.

Although probabilistic matching isn't as accurate as deterministic matching, it often uses deterministic data sets to train the algorithms and increase accuracy.

This process involves exposing the algorithms to a small group of deterministic and probabilistic data sets (a couple hundred thousand) and training them to make connections (identify the same user).

Then, the algorithms are applied to hundreds of thousands or even millions of data sets that don't contain deterministic matching.

Even though probabilistic matching lacks the accuracy of deterministic matching, the main benefit is that it offers better scale and reach.

However, There are a few downsides to probabilistic matching, including:

- Lack of transparency of the matching methods and accuracy.
- Redundant and outdated data.
- Decline in the availability of the data due to data-protection and privacy laws, such as the GDPR, requiring consent to collect IP addresses, location and other data (*more on this below*).

What Are Deterministic and Probabilistic Matching Used For?

Because deterministic and probabilistic matching aim to identify users across different devices and apps, their main use cases are **cross-device targeting** and **cross-device attribution**.

Cross-device targeting: Identifying users across different devices and showing ads based on their behavior on different devices – e.g. which websites they visit and what products they purchase.

For example, a user might view a jacket on a laptop and then see the same jacket or similar product in an ad on their smartphone.

Cross-device attribution: Similar to cross-device targeting, this focuses on attributing impressions and clicks to conversions and purchases made on different devices.

For example, if a user clicked on an ad for running shoes on their smartphone, but purchased them on their laptop, cross-device attribution would be able to attribute the ad click on the smartphone with the purchase on the laptop.

The Main Challenges With Identifying Users on Web Browser and Mobile Apps

As we've mentioned throughout this chapter, AdTech companies face a number of challenges with identifying users across web browsers and mobile apps.

The table below highlights the main challenges.

Challenge	Impact
The GDPR	Proper GDPR compliance requires companies to collect voluntary and explicit consent from users before they can save cookies to their device and collect personal data (IP address, device fingerprints, etc). The impact of the GDPR depends on a company's compliance policies, meaning companies will only be impacted if they decide to adhere to the GDPR's rules regarding valid consent.
The ePrivacy Regulation	Although it's currently being drafted, the ePrivacy regulation may have a bigger impact on user identification than the GDPR. For example, there's a chance that the ePrivacy regulation will require web browsers to be the gatekeepers of consent by allowing users to state their preferences in the browsers' settings. The impact of this may be similar to that of Safari's ITP, Firefox's ETP, and plugins like AdBlock Plus and Ghostery.
Privacy Settings in Web Browsers	The impact of privacy settings in web browsers varies. Safari and Firefox have the strictest privacy settings, with both browsers blocking third-party cookies by default, which eliminates behavioral targeting, cookie syncing, frequency capping, measurement and attribution. They also restrict device fingerprinting. Safari also puts limits on first-party cookies and local storage. Google Chrome is set to implement new changes in February 2020, which will give users more control over how third-party cookies are set and also block device fingerprinting. Chrome plans to stop supporting third-party cookies by 2022.
Browser Plugins (e.g. AdBlock Plus and Ghostery)	Ad-blocking plugins like AdBlock Plus and Ghostery are gaining popularity among internet users and have a similar impact on online advertising as privacy settings in web browsers. Most ad-blocking plugins prevent certain content (e.g. ads) from being displayed, which means advertisers can't reach their target audience and publishers don't earn ad revenue. Some popular ad-blocking plugins like AdBlock Plus allow users to whitelist certain websites, allowing them to display ads and earn ad revenue.

Solutions to the Identity Problem

Due to the direct and severe impact privacy laws and privacy settings are having on identity in online advertising, and the inefficiencies of cookie syncing, various companies and groups have proposed numerous ID solutions.

The main goals of these ID solutions are to:

- Identify users on web browsers as they move from website to website.
- Reduce page-load latency caused by cookie syncing.
- Compete with the walled gardens of Google and Facebook that have access to deterministic data and can offer advertisers better targeting, measurement and attribution.

There are many companies that are providing solutions to the ID problem, but here are the main ones:

[The Trade Desk](#) offers AdTech and data companies free access to its [Unified ID solution \(TTID\)](#), which is hosted under the adsrvr.org domain. In July 2020, The Trade Desk revealed that it would be [releasing a new version](#) of its Unified ID solution. This newer version of Unified ID, often referred to UID2, is open source and can be used by all companies, not just those working with The Trade Desk, and will be underpinned by hashed and encrypted email addresses.

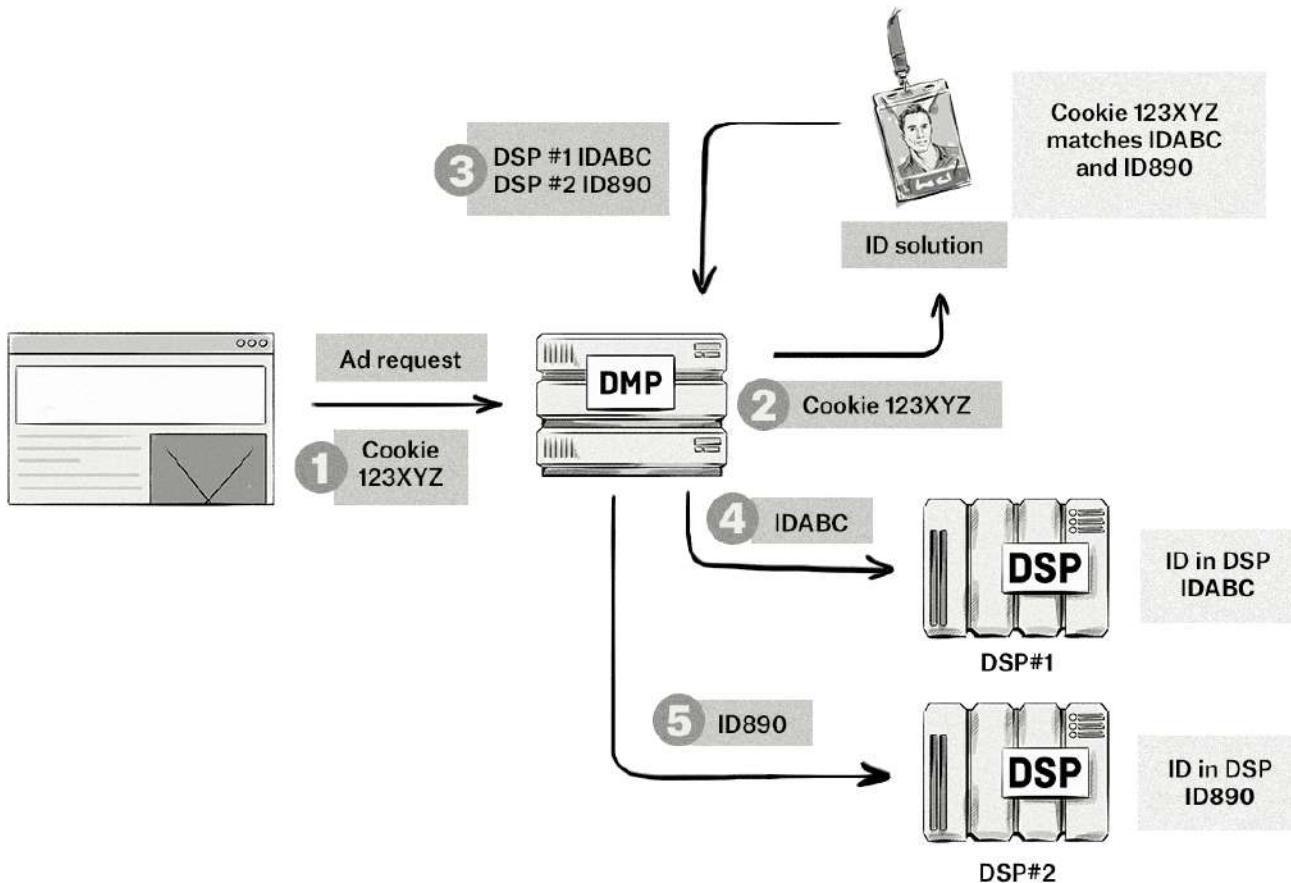
The [Advertising ID Consortium](#) is powered by the LiveRamp ID and hosted under the AppNexus domain, even though AppNexus withdrew from the consortium when it was acquired by AT&T in August 2018.

[ID5](#) is a company that allows publishers, data companies and AdTech vendors to outsource their cookie syncing processes with their partners and use ID5's cookie-matching table.

The [Secure Web Addressability Network](#) (SWAN), aka [SWAN.community](#), is another ID solution that is very similar to UID2, but with a few differences. The main companies behind SWAN.community are [Zeta Global](#), [51Degrees](#), [Open X](#), [ENGINE Media Exchange \(EMX\)](#), [PubMatic](#), [Rich Audience](#) and [Sirdata](#). On the 31st of March, 2021, SWAN began a 60-day consultation period whereby companies can provide feedback on the modal terms. SWAN is expected to go live in the middle part of 2021.

How Do These ID Solutions Work?

Most of the ID solutions work similarly to each other and act as an ID distribution and retrieval service. They manage the cookie-syncing and ID-matching processes on behalf of different AdTech platforms, so instead of DSPs and SSPs having to sync cookies between themselves, they could centralize the process via an ID solution.



Step-by-step explanation:

1. The browser sends an ad request to a DMP with the cookie ID of the user.
2. The DMP sends the cookie ID to the ID solution and aims to match it with existing IDs.
3. In this case, the cookie ID matches two IDs belonging to DSPs that the DMP has a partnership with.

4. The DMP sends the IDs from the ID solution to its DSP partners. The DSPs use the IDs from the DMP to identify which audience the user belongs to and then bid accordingly.

Although these ID solutions solve some of the challenges related to identity in AdTech, they don't provide a complete solution and are still impacted by privacy laws and privacy settings.

ID and Device Graphs

Apart from the ID solutions mentioned above, there are many companies that offer ID resolutions services like ID and device graphs.

The main goal of these solutions is to piece together IDs from online and offline channels to create a centralized view of consumers, rather than to use these IDs for online media buying.

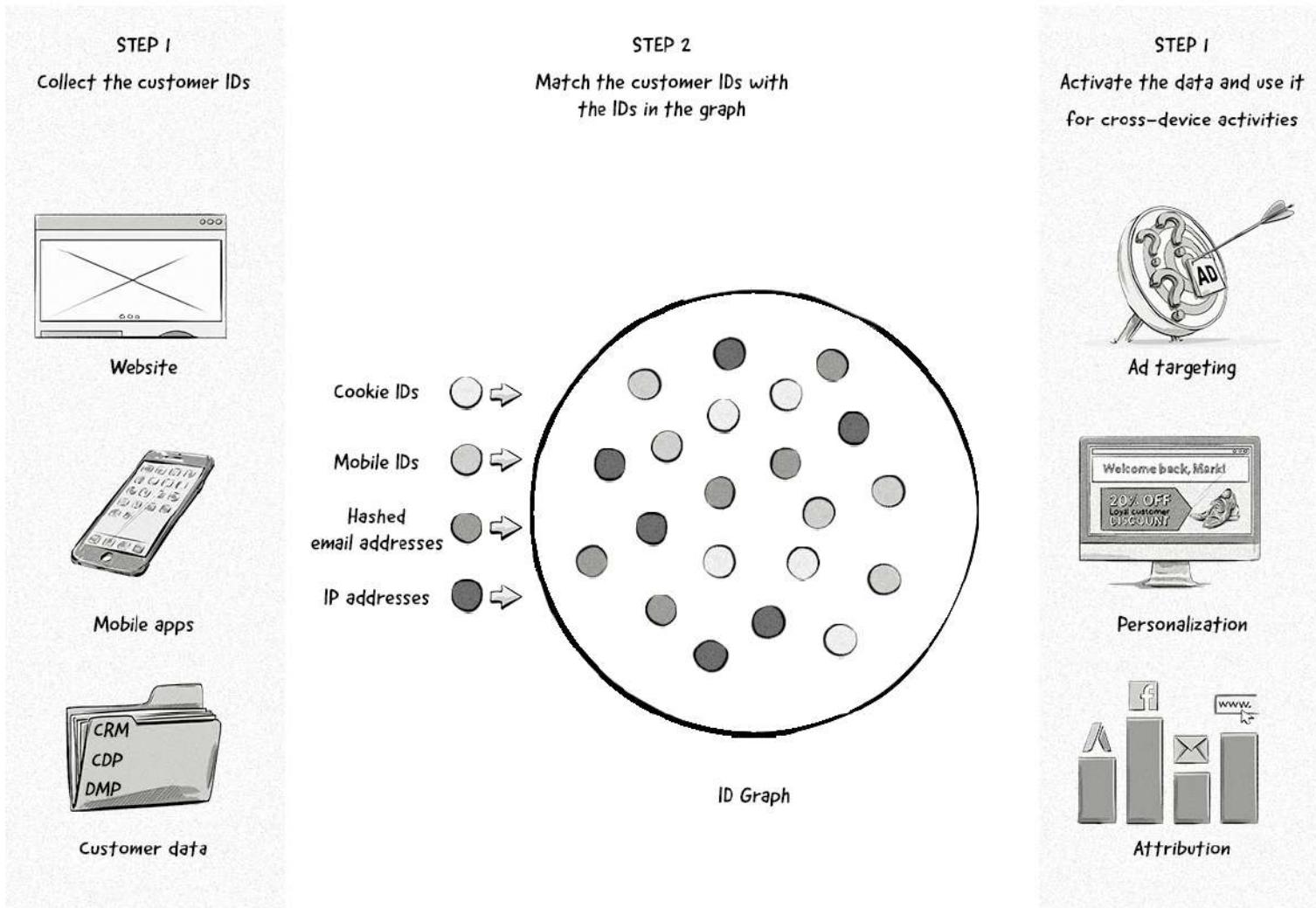
Below are just some of the companies that provide ID and device graphs:



How Do ID Graphs Work?

Here's an explanation of how ID graphs work:

How ID Graphs Work



Step 1. Data collection: A company would send its customer IDs (i.e. first-party IDs) to the ID graph. These first-party IDs could be taken from websites, mobile apps, and customer and data platforms (e.g. CRMs, CDPs, and DMPs).

Step 2. Match the customer IDs with the IDs in the graph: The company's first-party IDs would then be matched with all the other IDs in the graph, which would be done using a combination of deterministic and probabilistic matching.

Step 3. Activate the data for cross-device activities: The company can now identify their customers across different devices and channels and run various cross-device activities, like ad targeting, personalization, and attribution.

The Challenges Facing These ID Solutions

Apart from the fact that some of the solutions don't scale in the same way as they once did (i.e. IDs created from hashed email addresses aren't as readily available as IDs stored in third-party cookies), all these identity solutions face the same challenges — they still revolve around identification and rely on some type of ID.

The reason this is a problem is because walled gardens like Google and Apple are constantly strengthening their products to make them more privacy friendly.

We've seen this with Apple's ITP and changes to IDFA, and even Google has made changes to how Chrome handles third-party cookies and is also planning on phasing them out in the near future (possibly by 2022).

AdTech companies are moving from one identification method to another, and it won't be long until Apple and/or Google make some change to their web browsers or mobile operating systems to prevent these identification methods.

For this reason, many folks in the industry believe that these ID solutions are rather short-term solutions. Many say that the future of digital advertising and marketing won't be done on an individual basis, but rather done in a privacy friendly way where individuals are not identified.

It's too early to say if and when identification will disappear completely, so in the meantime, companies need to use an identity solution like the ones listed above to ensure they can still run effective advertising and marketing campaigns.

The Future of User Identification in Web Browsers and Mobile Apps

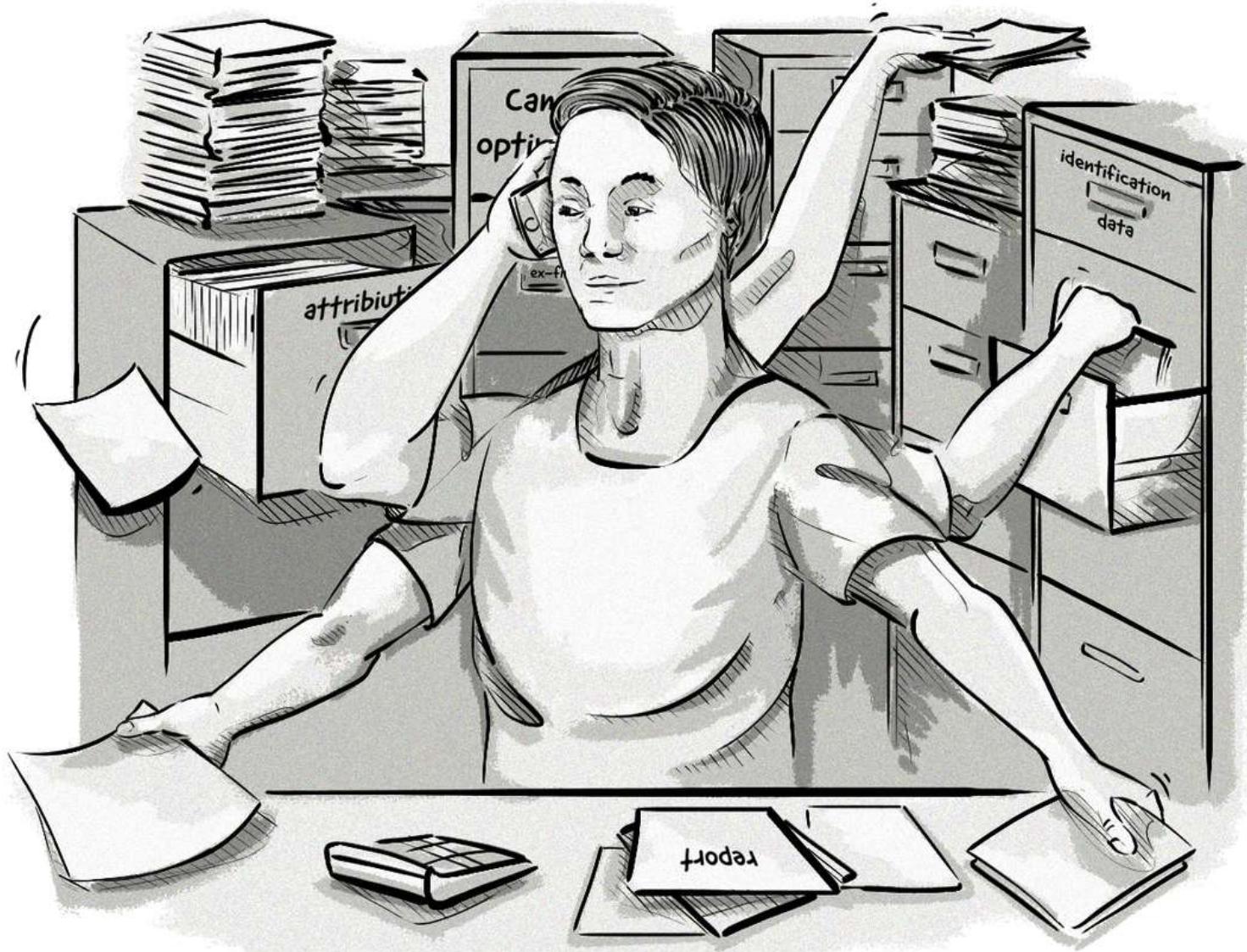
The end of third-party cookies in web browsers means that companies will need to change the way they identify users to continue powering key AdTech processes, such as behavioral targeting and measurement.

Several possible solutions have been proposed, including using email addresses as an ID and utilizing local storage, but many are limited to one domain and therefore won't be useful for cross-site identification.

At the moment, there's no clear alternative to third-party cookies or standards that can be applied by all companies in the digital advertising ecosystem. But initiatives like the [IAB's Rearc Project](#) will help bridge this gap.

Similarly, the future of mobile identifiers also looks bleak with many folks in programmatic advertising suggesting that it's only a matter of time before Google and Apple turn off their mobile IDs.

11. Data Management Platforms (DMPs) & Data Usage



So far in this book we've looked at the role advertising technology platforms play in creating, running, and optimizing digital ad campaigns.

Now we'll look at one of the most important elements that ties these two areas together: Data.

Data is the fuel that powers AdTech platforms and campaigns.

Specifically, data in digital advertising can be used for:

- Identification
- Targeting
- Reporting

- Attribution
- Campaign optimizations

Thanks to the rise of the Internet, advertisers and publishers now have access to enormous amounts of quality and generalized data sets that could never have been generated in the offline world. These data sets can give companies deeper insights into consumer behavior, identify trends, and improve campaign performance.

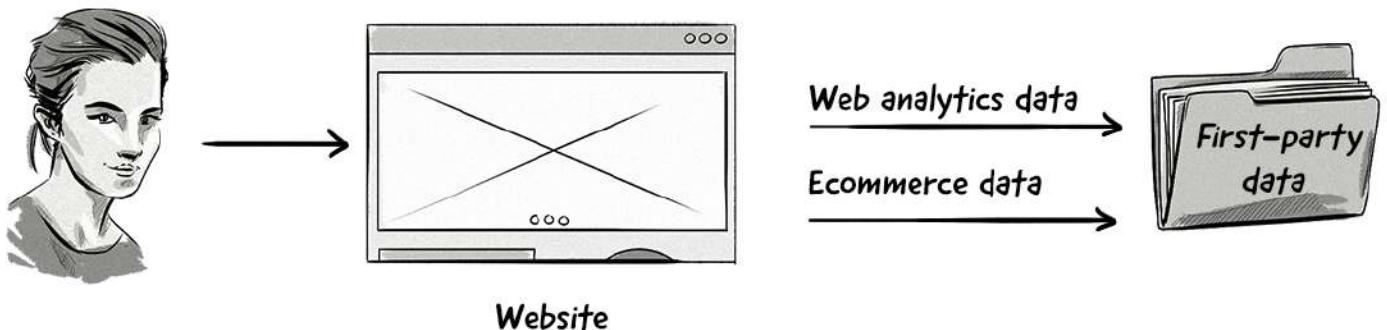
In this chapter, we'll look at how companies collect data, the different types of data, the role of data platforms like data management platforms (DMP) and customer data platforms (CDPs), and what data is used for.

The Different Types Of Data: First-Party, Second-Party, And Third-Party Data

Not all data is the same, and each piece plays a different role for both advertisers and publishers.

First-Party Data

First-party data is considered the most valuable type of data for both advertisers and publishers because it is collected directly from people who have interacted with the brand, such as customers.



First-party data is collected by a website or mobile app directly from the visitor/user.

First-party data is often collected by:

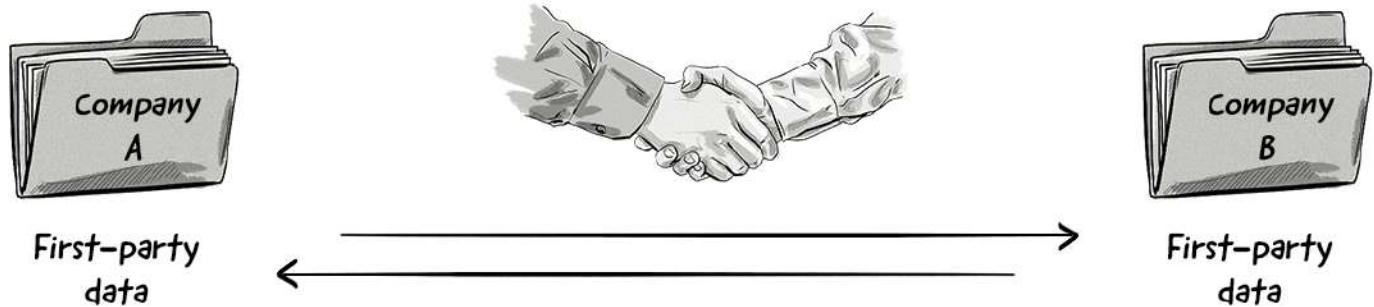
- **Ecommerce and offline transactions:** Data about which products people have purchased and the value of orders, as well as personal information such as names, postal and billing addresses, email addresses, and phone numbers.
- **Customer relationship management (CRM) systems:** Data about people who have created an account with your business, downloaded a digital product (e.g. ebook), and purchased something from you. Just like with ecommerce data, this often includes names, addresses, phone numbers, and email addresses.
- **Website and mobile app analytics:** Data about which pages the user has browsed, videos they've watched, and other content interactions.

First-party data can come from online and offline sources (see the section below for more details).

Brands and advertisers use this type of data to convert visitors into customers and upsell products and services to existing customers.

Second-Party Data

Second-party data is sometimes referred to as partner data, as it is first-party information collected by one company and sold or traded to another.



Second-party data is collected through data partnerships.

A typical partnership involves two non-competing companies with similar audiences.

For example, a hotel chain could partner with an airline and buy or trade the airline's first-party data. The hotel chain could use the airline's data to run targeted ad campaigns and display ads promoting their hotels to the airline's customers.

This partnership would benefit the hotel chain, as accommodation is often something people search for when booking flights.

The partnership could be one-way (i.e. the hotel chain buys the airline's first-party data), or the hotel chain and airline could set up a data-trade deal where they share information with each other.

This would allow the airline to display ads and messages to the hotel chain's customers as well.

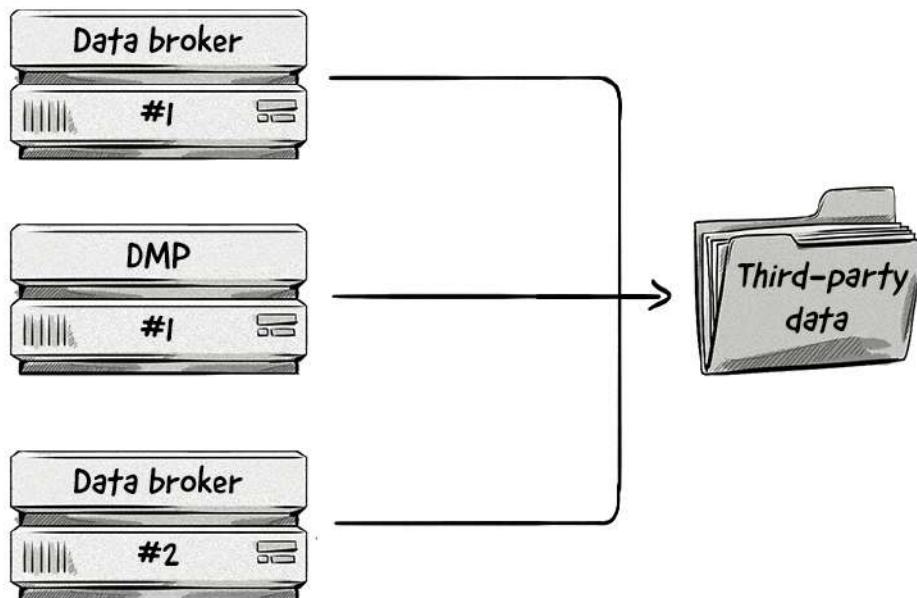
As the airline collects a lot of valuable first-party data, they could partner with many other types of companies, such as with exclusive brands that could target the airline's high-income customers with luxury products like watches and jewelry.

While first-party data is more valuable, as it contains people who either are existing customers or have expressed interest in becoming one, second-party data allows brands and advertisers to reach a new, untapped group of potential customers.

Third-Party Data

In terms of value, third-party data comes in last place. It is neither collected from the advertiser or publisher directly and isn't provided via a data partnership agreement.

However, third-party data still adds value to marketing and advertising campaigns and provides a couple of advantages over first- and second-party data, with the ability to reach a much bigger audience being the main one.



Third-party data is collected from a range of different sources.

Third-party data is usually supplied by data brokers or is added as a layer by a DMP vendor.

Many publishers and merchants monetize their data by adding third-party trackers to their websites or tracking SDK to their apps and passing data about their audiences to data brokers and DMPs.

This data can include a user's browsing history, content interactions, purchases, profile information entered by the user (e.g. gender or age), GPS geolocation, and much more.

Based on these data sets, data brokers can create inferred data points about interests, purchase preferences, income groups, demographics and more.

The data can be further enriched from offline data providers, such as credit card companies, credit scoring agencies and telcos.

From there, data brokers and DMP vendors can create audience segments.

Audience segments are made up of user profiles, which consist of various pieces of information, such as interests, location, and demographic information (e.g. gender and age).

*Check out the **Data Normalization and Enrichment in a DMP section** located later in this chapter for more information about user profiles and audience segments.*

A Comparison Of The Value Of First-, Second-, And Third-Party Data

Below is a comparison that illustrates how the different types of data stack up against each other.

	First-party data	Second-party data	Third-party data
Relevance and transparency	<p>★★★</p> <p>First-party data is made up of consumers that either are existing customers or who have engaged with a brand or publisher, meaning the audience is usually already part of the advertiser's target audience.</p> <p>This existing connection is useful for activities like up selling, cross-promoting, and returning sales.</p>	<p>★★☆</p> <p>Second-party data from one partner quite often contains audiences that share similar characteristics to the second partner's target audience.</p> <p>For example, an audience created by a luxury hotel would also match the target audience of a luxury watch brand.</p> <p>Given the direct relationship, it is usually fully transparent where the data comes from and how it was collected.</p>	<p>★★☆☆</p> <p>Because third-party data is collected and aggregated from different sources, the direct connection between an advertiser and user is lost. This means the relevance is often low.</p> <p>Also, most data brokers and DMPs provide little to no transparency over how they create data segments.</p> <p>The risks are that some pieces of data might be outdated or inaccurate because of extrapolation and lookalike modelling.</p> <p>However, given the sheer number of data sets, it may provide information that isn't available with first-party and second-party data, such as purchase preferences and income group.</p>
Accessibility	<p>★★★</p> <p><i>How easy is it for an advertiser to collect?</i></p> <p>As first-party data is collected directly from the brand or publisher's website or app, it is the easiest type of data to collect.</p>	<p>★★☆☆</p> <p>Second-party data requires data sharing agreements and systems integration for each partner, thus making it a time-consuming activity.</p>	<p>★★☆☆</p> <p>Once an integration with a DMP or a data broker has been established, you can buy data sets on demand without the need for additional implementation.</p>
Competitiveness	★★★	★★☆☆	★★☆☆

<i>What competitive advantage could this type of data provide?</i>	As first-party data is exclusively available to the brand or publisher, it can be used for high-converting activities, such as content and ad personalization.	Second-party data can be shared exclusively, meaning it can be used as a competitive advantage over other companies offering the same products or services.	As third-party data is usually widely accessible, many companies have access to the same pieces of data, meaning third-party data provides less of a competitive edge.
Reach <i>How many people could an advertiser reach by using this type of data?</i>	★★★ First-party data is limited to the visitors of the website (i.e. their online audience) and existing customers (e.g. offline CRM data).	★★★ Although it offers more reach than first-party data, second-part data is still limited to the partner's audience.	★★★ As data brokers and DMPs aggregate data from multiple partners, they have data on almost every user on the Internet. In practice, the audience is many times bigger than first- and second-party data sets combined.

As you can see from the table above, first-party data is by far more valuable than second- and third-party data in most areas.

Where Is Data Obtained?

Brands, advertisers, marketers, and publishers gather data from a range of online and offline sources.

Online Sources

Companies collect huge amounts of online data from a variety of sources, mainly:

- Analytics tools
- Customer-relationship management (CRM) systems
- Enterprise resource planning (ERP) systems
- Marketing automation platforms
- Mobile and web apps
- Campaign analytics

Offline Sources

Offline data can be collected from the following sources:

- Point of sale (POS)
- Offline CRM and ERP systems
- Transactional data

As all of the above data is collected directly from the user, it is classified as first-party data.

The types of data listed above are usually stored in various databases, which can either be the advertiser's or marketer's databases, or the software vendor's databases.

Combining Online and Offline Data Together

Companies that collect both online and offline data would combine them together to get a clearer picture of their customers and audience.

For large companies, such as retailers, integrating their offline and online records is not an easy task, but once it's done, it can prove valuable as it provides several business advantages.

If, however, a company collects small amounts of offline data (e.g. only email addresses), it is possible to just import the data into a database or DMP. But if a company collects large amounts of offline data, then they will need to onboard it into a data platform like a DMP or CDP.

See the **First-Party Data Onboarding section** below for more information.

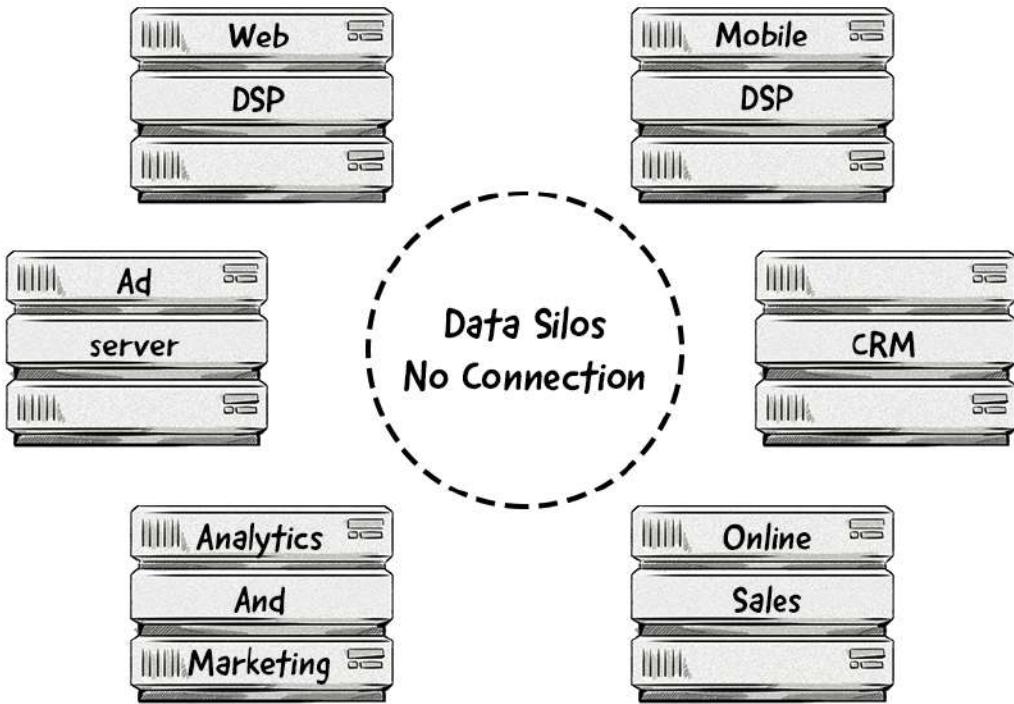
The Data Fragmentation Problem

While collecting vast amounts of data from multiple sources allows advertisers to improve campaign performance, the data is often stored across multiple tools and platforms. These individual databases are often referred to as *data silos*.

What is a data silo?

A data silo is a collection of data controlled by one department (e.g. sales) and isolated from other departments within an organization.

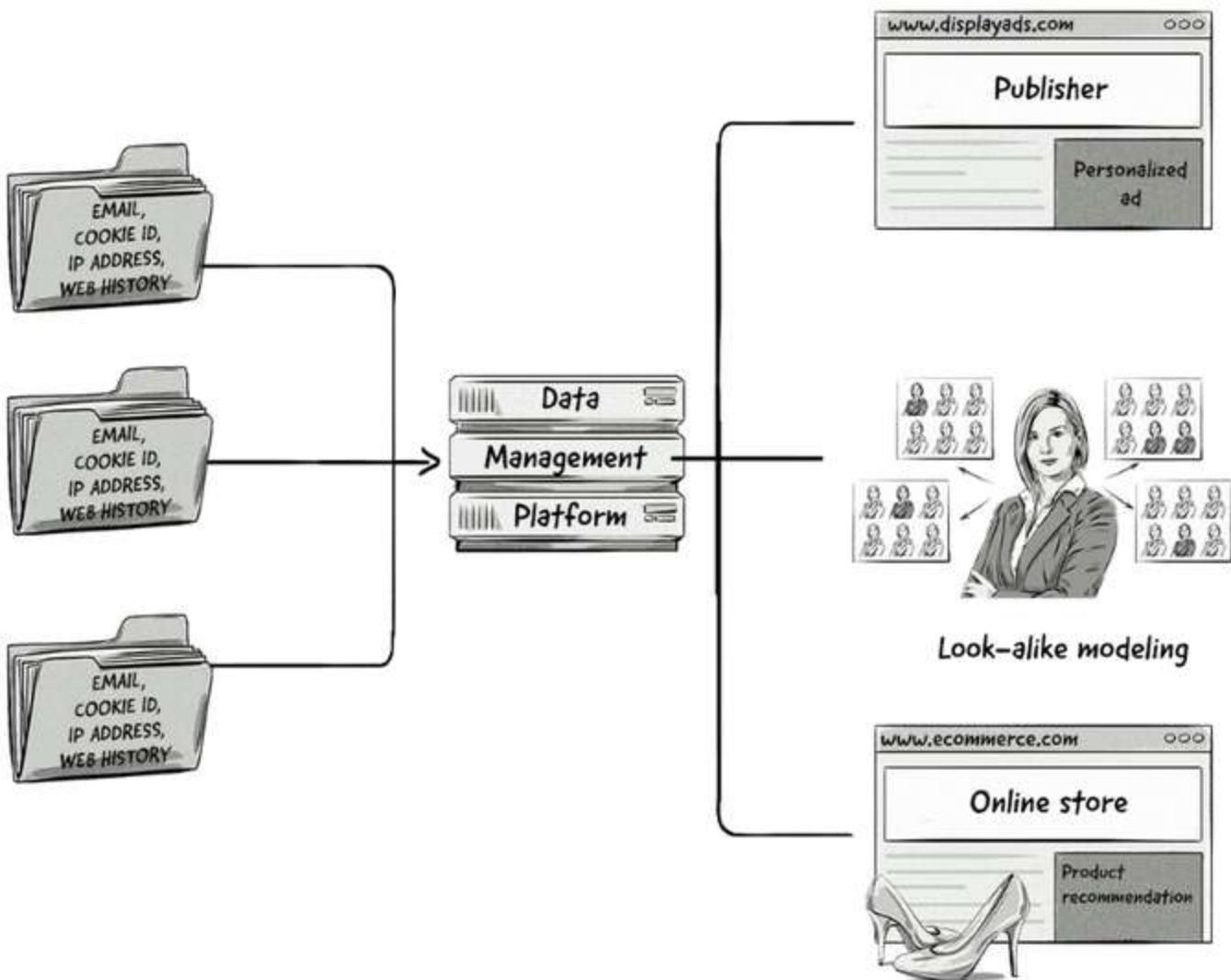
The main disadvantage of having data silos is that the data from different departments (or systems) cannot be integrated together, which restricts the data's full potential from being realized.



Data silos are individual databases that are not connected with one another.

Having data stored in different silos means that advertisers can't see the full picture of their target audience or campaigns' performance, which often leads to poor decision-making, missed opportunities, and ad waste.

The solution to this problem is a **data management platform (DMP)**.



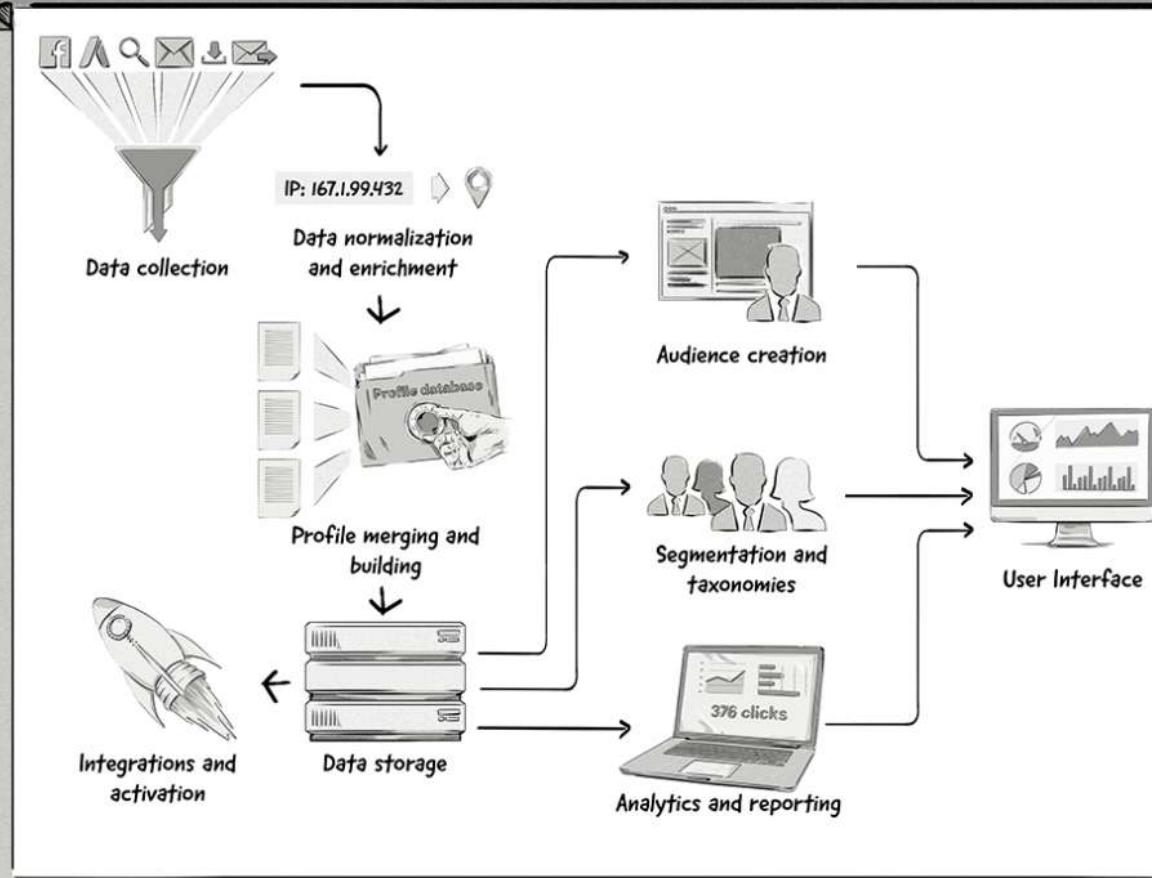
Data Management Platform (DMP)

As we've touched on previously, a data management platform (DMP) is a technological platform used to collect, store, analyze, segment, and activate data.

In this section, we'll look at the main functions of a DMP and uncover some of its potential use cases.

Here's a look at the processes and components of a DMP:

The Anatomy of a Data Management Platform (DMP)



Let's take a closer look at these components and processes.

It's worth noting that the below processes can also be carried out by other data platforms like customer data platforms (CDPs), which we cover towards the end of this chapter.

Data Collection in a DMP

Collecting data can be done in a few different ways, depending on where the data is stored.

Pixels and Tags

Probably the simplest way for a DMP to collect first-party data is by adding a 1×1 transparent pixel (also known as a tag or tracking pixel) to your website.

The pixel itself is just a piece of HTML. When the pixel loads on a page, it sends off a request to the DMP to retrieve the 1×1 transparent image.

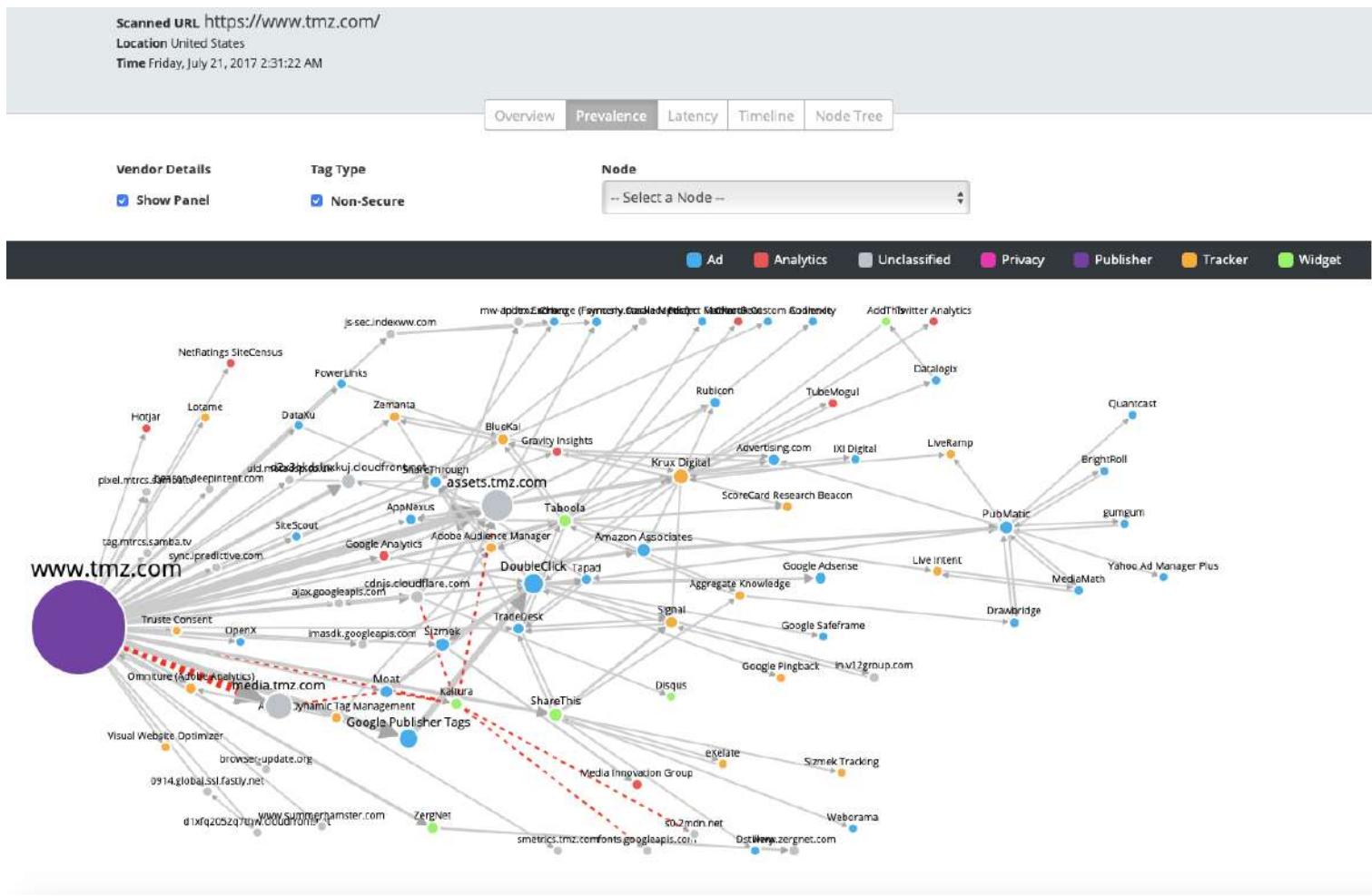
Once the DMP has returned the 1×1 pixel, it can assign a cookie to the user and store it in their browser. The information in the cookie can then be passed to the DMP.

Piggybacking

Piggybacking is when we insert a single master pixel on a site's pages which can either contain or trigger multiple tracking pixels from various sources and networks that are not placed directly on the site.

When the master pixel loads, it subsequently loads the other pixels.

The images below illustrate the piggybacking process:



Piggybacking advantages	Piggybacking restrictions
One pixel can consolidate all third-party pixels.	Image pixels can only piggyback off one image pixel.
A single pixel keeps everything clean and organized.	JavaScript pixels can actually piggyback off an unlimited number of JavaScript and image pixels, but too many piggybacked pixels could slow down the user's browser.
Data is tracked more accurately across all marketing channels.	Insecure (http://) pixels can only be placed on an insecure page — i.e. they can't be placed on pages with https:// .
It reduces the need for web developers to be involved in	Publishers don't have control over the piggybacked

implementing pixels on a site.	pixels, which can lead to problems around privacy and complying with data protection laws like the GDPR.
--------------------------------	--

Tags

Tags are pieces of JavaScript or an iframe. Just like with pixels, tags are added to a website and when loaded, send a request to a DMP. The DMP responds to the request and places a cookie in the user's browser and collects data.

Sometimes, publishers will use a tag management system (TMS) to control and manage the various JavaScript snippets and pixels they have on their website. These tags and pixels are placed in a container which is inserted into a website's pages, usually directly under the opening body element <body>.

The main benefit of a tag manager is that publishers can easily add, remove, and modify their HTML tags, JavaScript snippets, and pixels from a single user interface, rather than having to ask their web developers to make manual changes in the website's HTML.

Application Program Interface (API)

APIs are used to exchange data between web servers and a DMP. This type of data exchange is ideal for companies that have a number of data silos as it allows them to efficiently collect data from different databases.

This form of data collection is also referred to as a server-to-server integration.

First-Party Data Onboarding

First-party data onboarding involves taking a company's offline customer data and integrating it with their online customer data.

So, for example, a company could have the following customer data in their offline database:

- Names
- Residential addresses
- Phone numbers
- Email addresses
- Dates of birth
- And all other data they have about customers in their offline customer relationship management (CRM) and transactional systems.

They could then onboard it with the data they have in their online databases, such as:

- Data from their web-analytics tools and ad servers.
- User account information (e.g. account information from the company's online payment system).
- Any other online information the company has collected about the customer, including the same information they've collected offline — e.g. name, email, and residential address.

Depending on the amount of offline data a company has, they might just be able to import the data as a CSV file. But if they have a large amount of data, which is often the case, then they would likely need to use a data onboarding platform like LiveRamp.

Here's a list of some of the most common data-onboarding platforms on the market:



The general process involves a company uploading offline data with an onboarding platform, anonymizing it to remove any personally identifiable information (PII), e.g. email addresses, names, physical addresses, etc., and matching the offline data with the company's online data.

How can data be anonymized?

Below are the most common ways to anonymize data and remove PII:

Hashing – irreversibly converting data into a non-human readable value.

Encryption – making the data accessible only to those with the decryption key.

Generalization – replacing a specific category with a more general one, for example, changing a user's age from 42 to an age range of 40-49, Starbucks Coffee Shop at Wrocław Market Place to a coffee shop.

Suppression – replacing attributes, or parts of them. For example, changing a zip code from 44340 to 44***, location from 51.1088316,17.032966 to 51.1*****,17.0*****

Adding noise – adding random values to numeric attributes in a way that their average remains unchanged.

Swapping the data – exchanging certain fields of one record with the same fields of another similar record, for example, swapping the ZIP codes of two records.

The definition of “anonymized data” varies among companies and countries.

In the USA, it generally means removing personally identifiable information like names, postal addresses, and email addresses.

However, under certain privacy laws, like the EU's GDPR, the term anonymized data means any data that can't be used to identify a person. So, even if a company just collects cookie IDs, device IDs, and IP addresses, this data is still classed as personal data under the GDPR because AdTech and MarTech platforms can still identify users using those pieces of data (e.g. identify returning visitors).

Data anonymization is done to mitigate exposure of PII, such as in the event of a data breach, and to comply with certain data protection and privacy laws.

However, under certain privacy laws, like the EU's GDPR, the term anonymized data means any data that can't be used to identify a person. So, even if a company just collects cookie IDs, device IDs, and IP addresses, this data is still classed as personal data under the GDPR because AdTech and MarTech platforms can still identify users using those pieces of data (e.g. identify returning visitors).

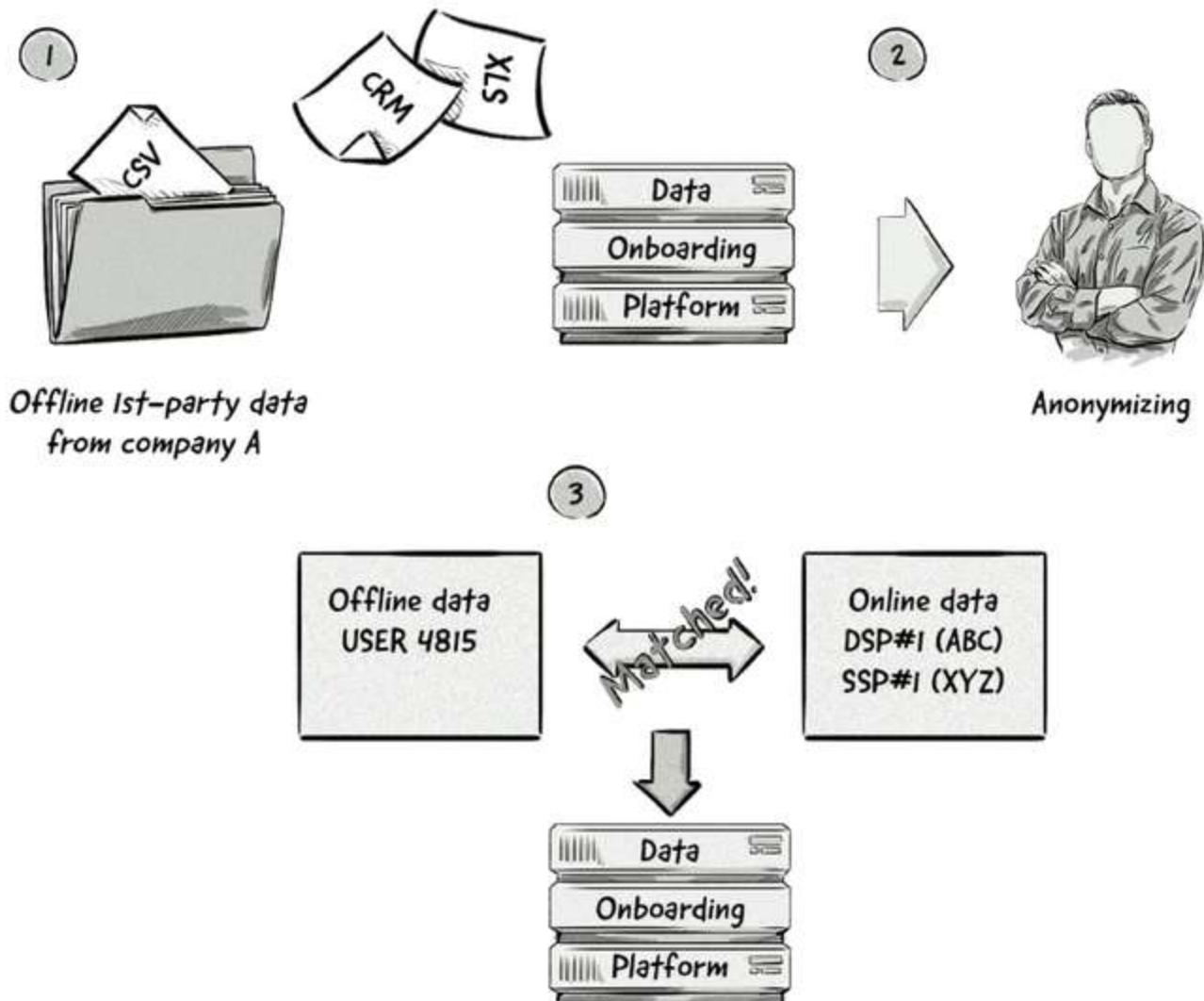
Data anonymization is done to mitigate exposure of PII, such as in the event of a data breach, and to comply with certain data protection and privacy laws.

How Does First-Party Data Onboarding Work?

While each data onboarding platform will handle the process differently, the basic principle is the same:

1. Companies upload their offline first-party data to the onboarding platform by importing CSV, CRM, and XLS data files
2. Through an anonymization process, the onboarding platform transforms the data to remove any personally identifiable information (PII).
3. The offline data is then matched with the online data with the help of identifiers. For example, if a company has collected a customer's email both offline and online, the onboarding platform would match the two sources of data via the common email address.

Here's a visual representation of the data onboarding process:



The first-party data onboarding process.

Data Onboarding With Google AdWords and Facebook Ads

Due to the vast amounts of data that is being onboarded via companies like LiveRamp, the process can be quite complex and take a number of days to complete.

Other companies, like Google and Facebook allow advertisers to upload simpler offline and online data sets (typically just an email address) to their platforms and use it for targeting and retargeting. Although this method doesn't offer the same scale as data onboarding via the companies above, it's often a suitable option for small- and medium-sized companies.

Google Ads

[Google's Customer Match](#) service allows companies to upload their audience data to Google Ads and target those customers, as well as related audiences, across Google's properties, including the Search Network and Google Shopping, YouTube, Gmail, and the Display Network.

The data that can be uploaded to Customer Match includes:

- Email
- First name
- Last name
- Country
- Zip code
- Phone number

Facebook Ads

[Facebook's Custom Audiences](#) works in a similar way to Google's Customer Match.

This service allows companies to not only upload customer email lists to Facebook Ads for targeting on the Facebook platform, but to also place a tracking pixel on their website and/or app. From there, the pixel will track that user and then display a customized ad or offer to that user on Facebook.

Data that can be [used to create a custom audience](#) in Facebook includes:

- Email
- Phone number
- First name
- Last name
- City
- State or province
- Country
- Date of birth

Data Normalization and Enrichment in a DMP

Once the data has been collected, it's time to normalize it.

The data-normalization process can include a number of the following actions:

- Gathering IDs from web cookies.
- Deleting redundant or useless data.
- Transforming the source's data schema to the DMP's data schema.
- Enriching the data with additional data points, such as geolocation and OS/browser attributes.

The data normalization and enrichment stage provide two main benefits:

1. It organizes the various data sets into a common format.
2. It improves data value and quality.

During the normalization and enrichment stage, each user will be assigned a unique ID and given different attributes, which will play a key role in the segmentation stage.

These attributes can include:

- Age
- Gender
- Location
- Browser history
- Interests
- Purchase history

Profile Building and Merging

A profile is a set of data collected from events tracked by a DMP. It represents a user and may contain the following pieces of information:

- profile id
- cookie id (list)
- hashed email (list)
- sid / uuid (list)
- country (last seen)
- name ([nullable](#))
- device_type (last seen)
- device_vendor (last seen)
- device_os (last seen)
- browser_vendor (last seen)
- gender (nullable)
- company (nullable)
- company size (nullable)
- matching ids (list)

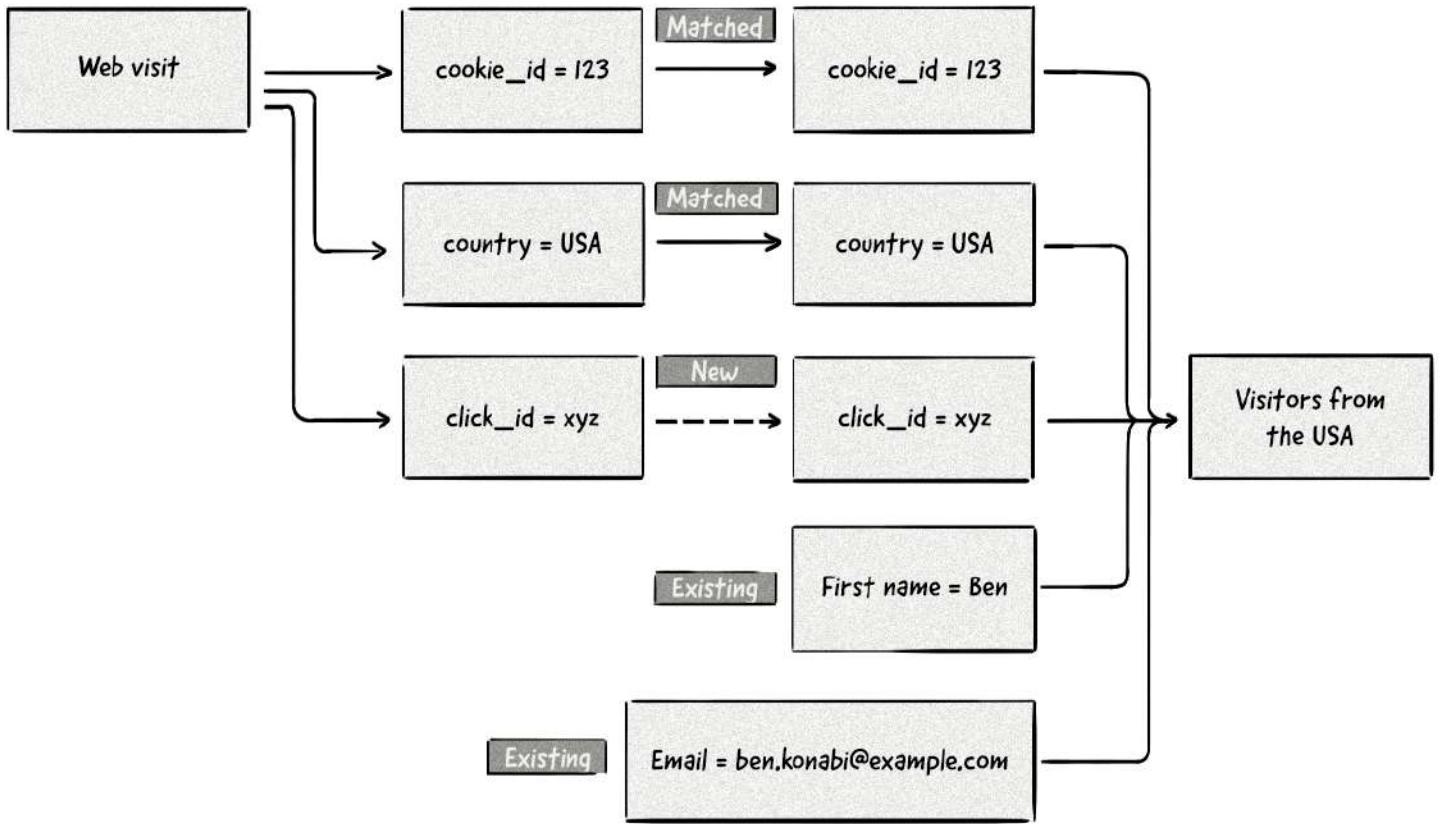
In some cases, a profile will be created containing only a few pieces of data (e.g. cookie id, device_type, and device_os) and will be extended when more data becomes available — i.e. **profile building**.

When a DMP receives new events containing a known piece of data (i.e. one that is in the DMP), then it is added to the relevant profile.

On the other hand, if an input event contains a new piece of data (i.e. one that isn't in the DMP), then a new profile is created.

It's quite often the case that two profiles contain the same pieces of data (e.g. cookie id).

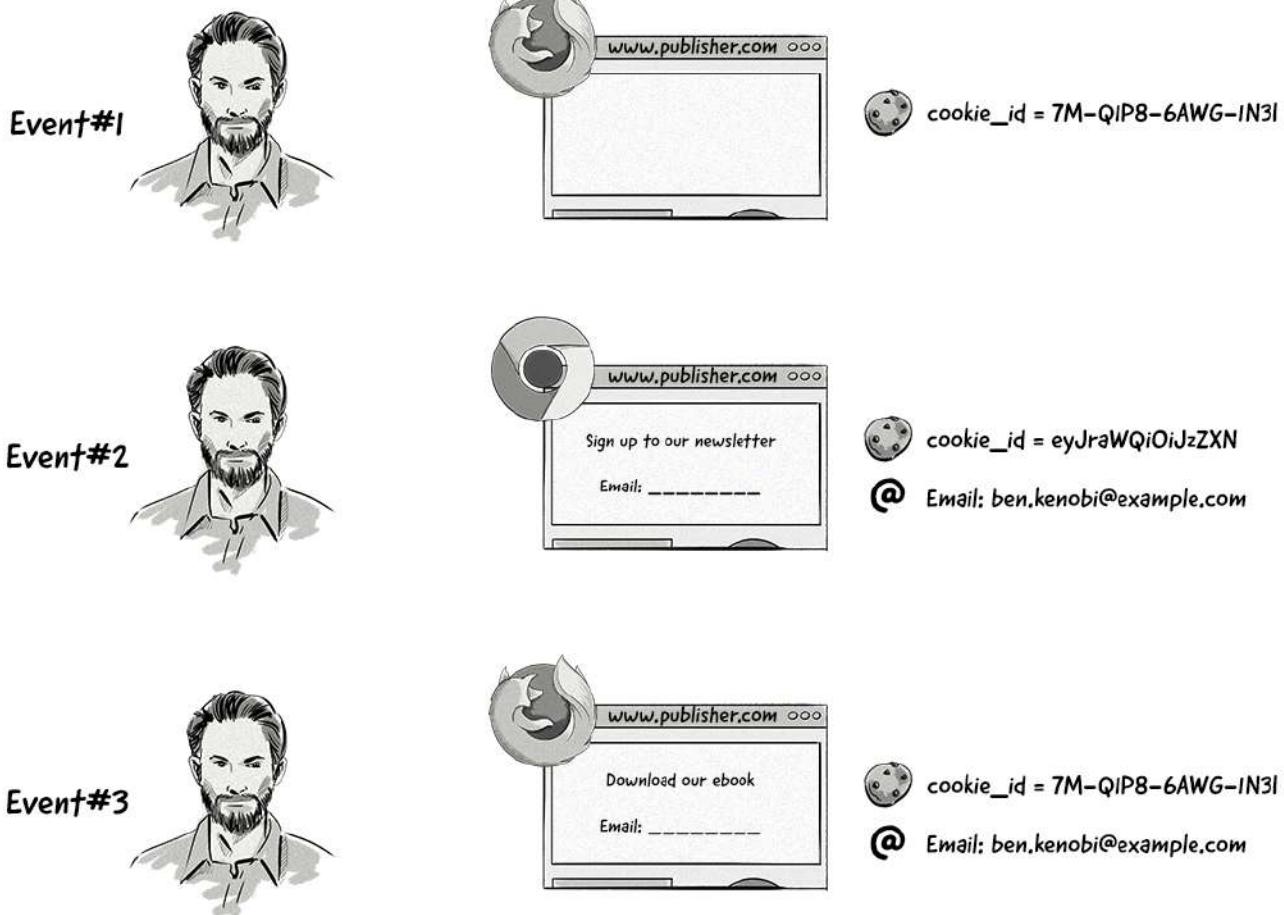
If this occurs, the DMP will have to perform an operation known as **profile merging**.



The image above illustrates how profiles and audiences are built in a DMP.

The goal of profile merging is to ensure that no profiles contain duplicate pieces of data and that no two profiles contain the same unique identifiers (e.g. cookie IDs and email addresses).

Let's look at the following example:



All three events come from the same user, but this isn't known until the third event arrives in the DMP, meaning all three events would be treated as separate profiles.

For this example, all three profiles would be merged together into one profile.

Most DMPs would use a master ID — a single ID associated with one profile — to ensure accurate profile merging. Most often this would be a persistent ID, such as an email address.

When new events containing the master ID enter the DMP, all other data associated with the event will be added to that profile.

How to Merge Profiles Together

There are a few ways a DMP can merge profiles together.

Below we'll list some of the main ways.

Overwrite existing IDs and attributes: This is one of the simplest ways to merge profiles as it simply replaces existing IDs with new ones as they enter the DMP.

Alphabetical sorting: This method sorts the values alphabetically and then uses the first value. For example, if there were 2 profiles with the names “Robert” and “Bob”, then “Bob” would be used as the name value because the letter “B” comes before “R”.

Timestamp sorting: With this method, the value that has the first or last recorded timestamp would be used.

In most cases, timestamp sorting will be the most desired method to use.

Wait-and-see sorting: A more complex approach would be to keep all values for reference until a different sorting method (e.g. timestamp) becomes available. Then you’d be able to see whether the assumption was correct and decide on the final values after the merging operation has finished.

Data Storage

Although the concept of storing data in a DMP seems rather simple, the actual technical implementation can be challenging due to the large amount of data being stored, as well as the need to move it to other areas and prevent data loss.

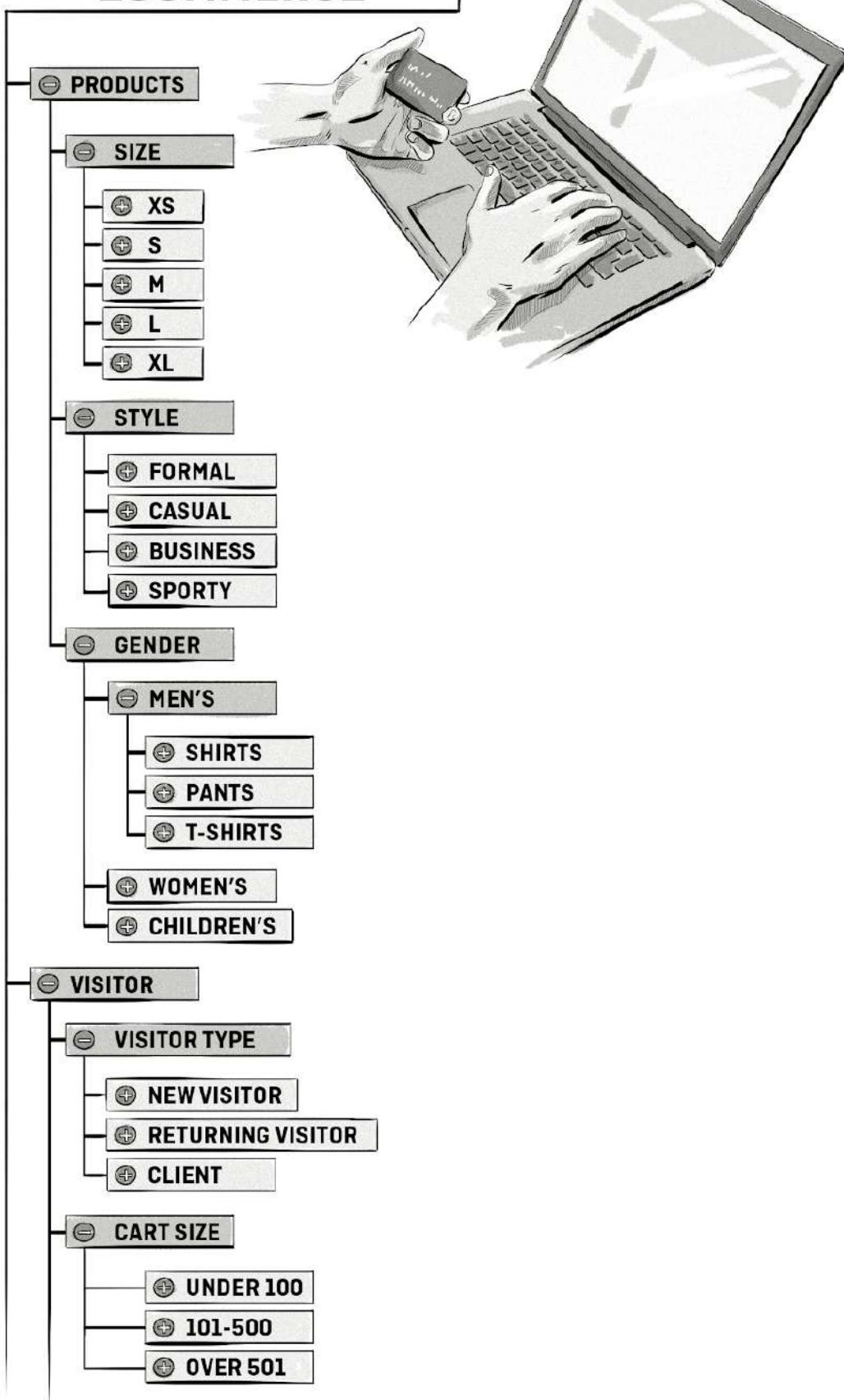
Data Taxonomies

Taxonomy in a DMP refers to the naming convention used for various pieces of data.

For example, instead of having two taxonomies like “user” and “visitor”, you could create or define one taxonomy (e.g. “user”) that represents both terms.

Below is an example of how an ecommerce store could structure its taxonomies:

ECOMMERCE



Audience Segmentation and Creation

Audience segmentation involves placing users into groups based on common characteristics, such as age, location, behavior, interests, and many others.

These segments form the basis for data activation, whereby these segments are used for a number of different purposes, such as for ad targeting and analytics.

See the **Use Cases Of Data Activation With A Data Management Platform (DMP)** section below for more details.

How A DMP Creates Audience Segments

To create audience segments, a DMP uses a series of conditions to filter the data and produce specific groups of users.

The conditions may include general information such as:

- Country, region, or city
- Device type
- Operating system
- Referral URL

And may also include more specific data about users' behavior like:

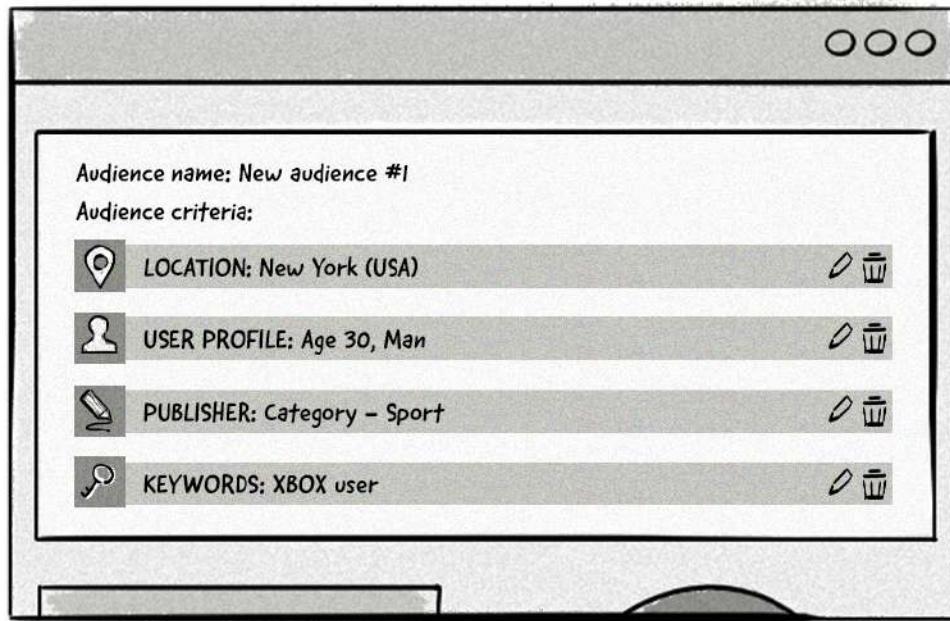
- Events (button clicks, page-views, etc.)
- Conversions (downloads, purchases, etc.)
- Ads viewed

It could also contain demographic data, such as:

- Relationship status: In a relationship
- Interests: Gardening
- Age group: 35-39
- Gender: Male
- Home Value: Between \$200k – \$400k
- Annual income: Between \$60k – \$90k

Advertisers can then combine multiple segments to directly target the audiences they want to reach with their online advertising campaigns.

Here's an example of what that might look like:



An example of how a DMP creates audience segments.

Apart from selecting which users to include in an audience segment, you can also add filters to exclude users from the segment and set the recency and frequency of certain actions.

For example, you could add users who have viewed your website at least 5 times (frequency) in the past 30 days (recency).

These two additional factors will go a long way towards defining your audience segments and their usefulness and can significantly impact the relevance and scope of the segments.

Relevance: Increasing the time frame for data points to be included. For instance, setting a time frame of "greater than 30 days" can add users who may be less likely to convert. However, raising the frequency to "at least 3 times" for certain event information can mean adding a user who is highly engaged and likely to convert.

Scope: Similarly, extending the time frame and reducing the frequency will broaden the scope of the audience, which would be useful for brand awareness but not for increasing conversions.

Once you've created audience segments, you can now **activate your data**.

Use Cases Of Data Activation With A Data Management Platform (DMP)

Data activation in a DMP is using audience segments for a range of different activities. It's often considered the most important function of a DMP.

Below are the most common ways advertisers and publishers can activate their data and audience segments in their DMP.

Data Activation for Advertisers

Media Buying And Optimization

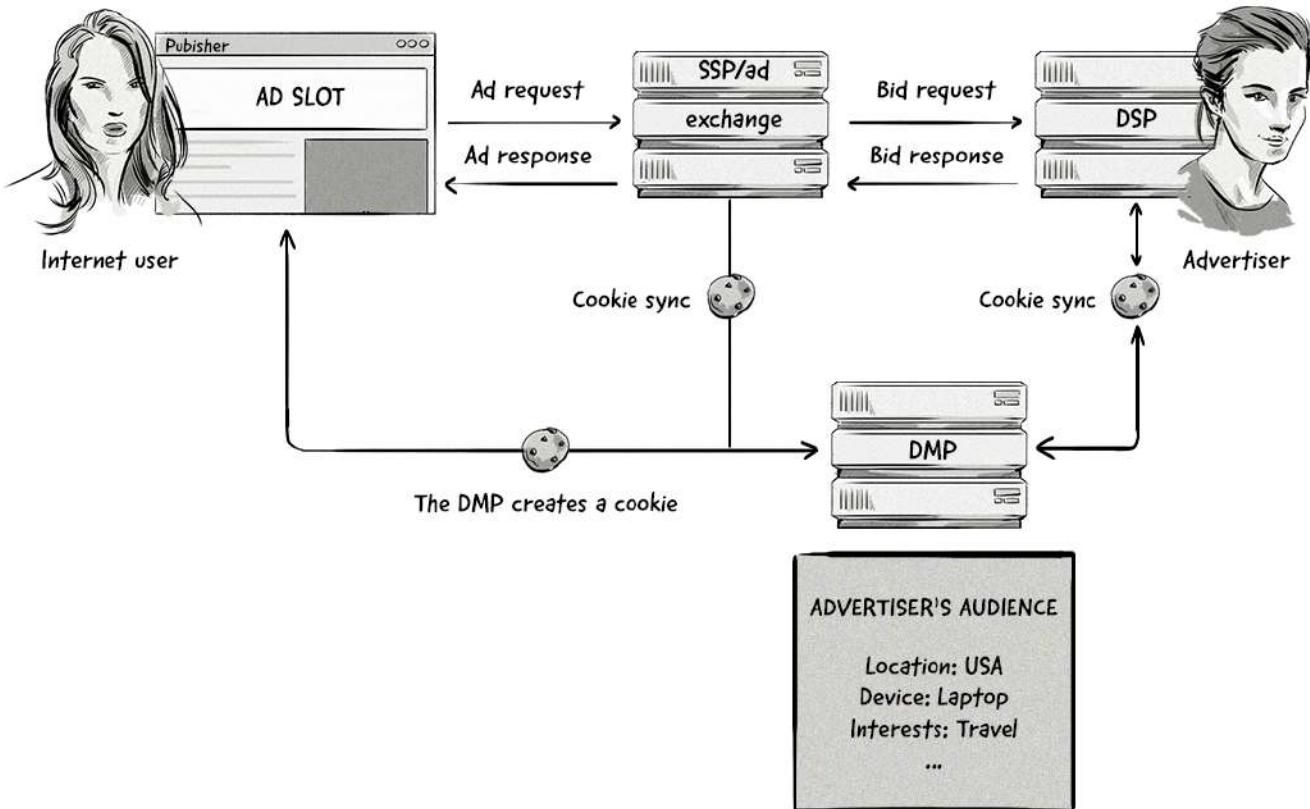
For advertisers and marketers, activating their data for digital media buying is one of the main use cases.

The main way to activate data for media buying is via [**cookie syncing**](#).

*We covered cookie syncing in a previous chapter: **10. User Identification***

First, the advertiser would start by integrating their DSP with a DMP. From there, the advertiser can create audiences and sync their cookies with the DMP's cookies so they can identify their audience across multiple publishers.

When an advertiser (via a DSP) identifies a user who belongs to one of their audiences, they can show them an ad that is more personalized and relevant. Because this form of targeting is more dynamic than traditional targeting (e.g. showing iphone users the same ad), it often produces more clicks and conversions.



It's important to note here that the DMP could either have its pixel on the publisher's website, or it could receive it from the SSP via piggybacking, or both.

Brands and advertisers can also use a DMP to improve retargeting and dynamic creative optimization.

Another key part of activating data in a DMP for media buying is improving campaign performance and reducing ad waste.

DMPs can provide advertisers with detailed reports, allowing them to see the best and worst performing audiences, and make real-time optimizations to increase reach, performance, and optimize media spend.

Look-alike Modeling

Advertisers can use a DMP to perform lookalike modeling — a process that finds people that have similar characteristics to an advertiser's target audience.

For example, an ecommerce store selling motorsport gear wanting to increase its audience could perform lookalike modeling to find new people who were interested in motorsports but hadn't visited their store. They could define a set of criteria that matched their existing audience, such as location and interests, and then use a DMP to create those new audiences.

The ecommerce store could also place a pixel from a DMP on their purchase confirmation page to collect data about customer behavior across different websites. The DMP could analyze this data and look for similarities in behavior among the store's existing customers. These similarities can then be used as the basis for creating new audiences.

How Does Look-alike Modeling Work?

Lookalike modeling analyzes data and uses algorithms to identify common characteristics and similarities in behavior.

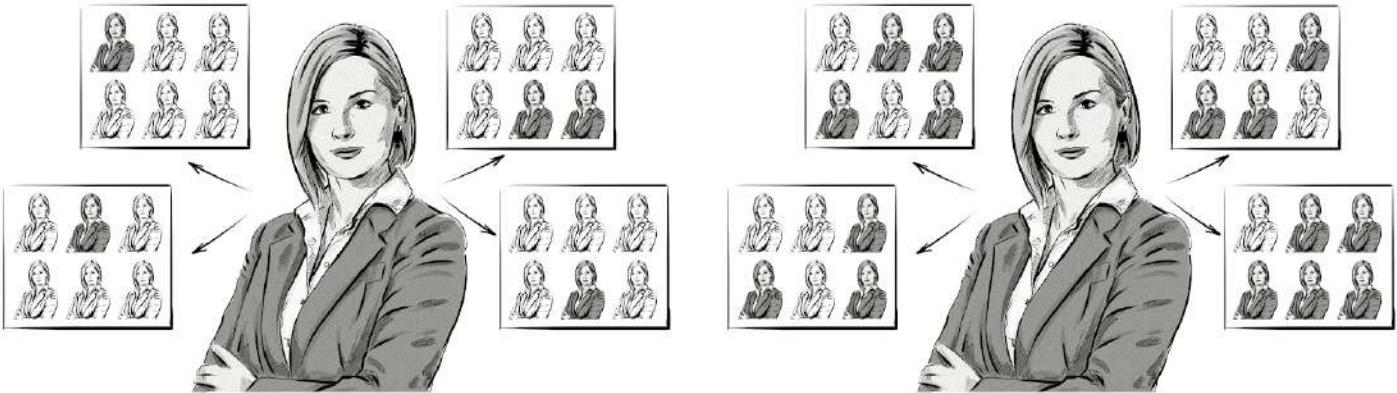
Because the main goal of lookalike modeling is to find new audiences, it works best when it's able to analyze data outside of an advertiser's own database. For this reason, most lookalike modeling is done by DMPs that have collected large amounts of data from multiple sources.

To create a look-alike model, advertisers need to define the attributes and behaviors of their most valuable customers.

The stricter the look-alike model is (i.e. the more attributes), the better chance advertisers have of finding more people who match their target audience. This will improve the advertiser's chances of receiving more conversions.

However, advertisers could be less strict with the look-alike model by defining fewer attributes and behaviors if their goal is to focus on reach and awareness rather than higher conversion rates.

Below is an example of a look-alike model that has tightly defined (more) attributes and behaviors, and one that has loosely defined (less) attributes and behaviors.



Attributes & behaviors of our best customer

- ✓ Average online purchase: >\$100
- ✓ Online shopping behavior: Often purchases cosmetics and perfumes
- ✓ Purchase frequency: Makes at least 2 purchases a month

Attributes & behaviors of our best customer

- ✓ Average online purchase: >\$20
- ✓ Online shopping behavior: Often purchases cosmetics, perfumes, clothes, jewelry, and hats.
- ✓ Purchase frequency: Makes at least 1 purchase every 3 months

TIGHTLY DEFINED ATTRIBUTES & BEHAVIORS

LOOSELY DEFINED ATTRIBUTES & BEHAVIORS

What Can Look-alike Modeling Be Used For?

The main use case of look-alike modeling is prospecting, which involves finding new potential customers and/or visitors.

However, it can also extend the reach of online advertising campaigns.

Let's say you target audiences based on a set of attributes, such as age, gender and location.

By applying look-alike modeling to your campaigns, you can find similar customers who perhaps aren't included in your current audiences because you don't have enough data (e.g. we lack the attributes needed to make a match) or they don't fit your current audiences (i.e. they consist of other attributes) but are still similar to your best customers.

Audience intelligence

Advertisers can enrich visitor and customer data by matching and comparing their current audiences against third-party data sets and adding information about both customers and prospects, including their demographics, interests, income or purchase preferences, to their database.

This allows them to learn more about how people behave, fine tune their target audience, and identify what makes them convert.

Brands and advertisers can use audience intelligence to optimize and personalize certain areas of their site and campaigns to improve engagement and increase conversions.

For example, a travel website that promotes thousands of different hotels and resorts may identify a group of visitors who are less price sensitive, but require more flexibility and display more expensive offers with a free cancellation option to them.

Data Activation For Publishers

So far, we've explained the ways in which advertisers can use a DMP for data activation, so now it's time to have a look at how publishers can utilize a DMP.

Similar to advertisers, the first step in monetizing their revenue is to create audience segments. From there, they can be used for a number of different use cases.

Here are the main ways publishers can activate their data.

Increase the Value of Their Inventory

Due to the large volume of user data that many medium- and large-size publishers collect, they can increase the value of their inventory by creating audiences and then offering them to advertisers.

The reason this benefits publishers is because advertisers will pay a higher price (e.g. CPM or CPC rate) if they know that their ad will be seen by the right target group and highly engaged users.

How are publishers able to pass these audience segments to advertisers?

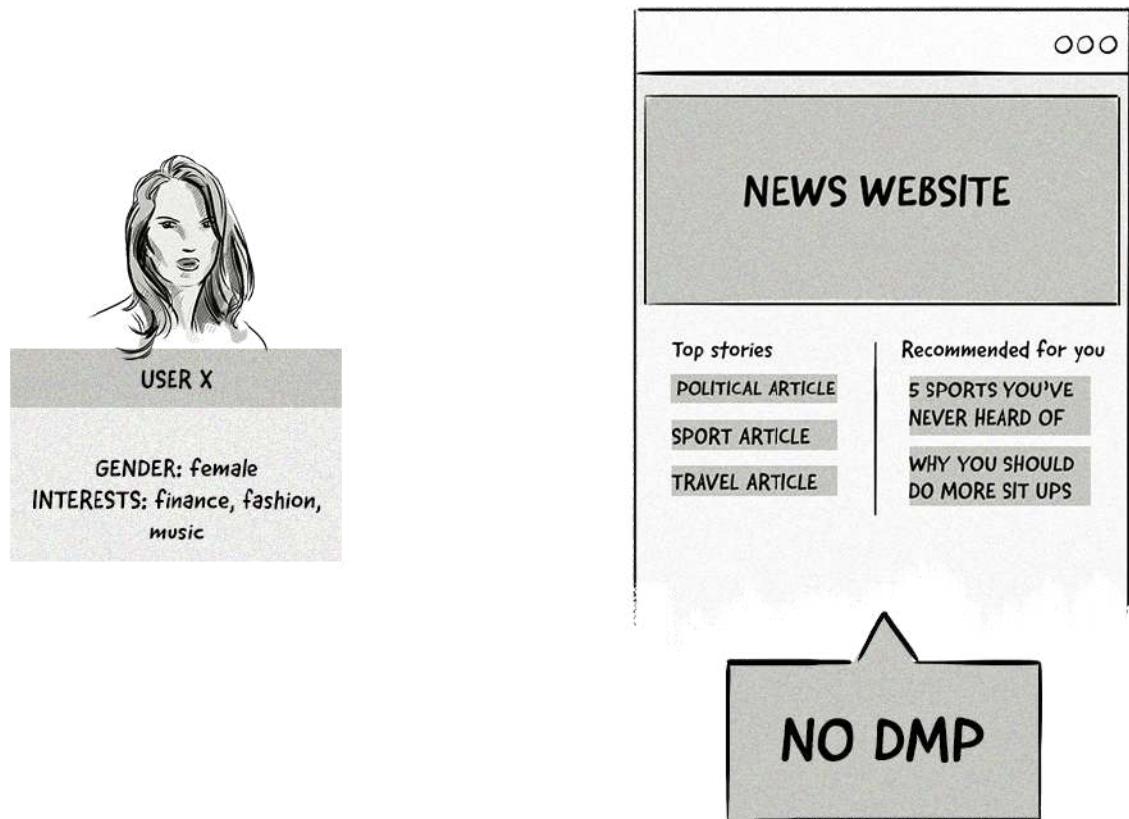
There are a few ways publishers can make their audience segments available to advertisers and increase their ad revenue:

1. **Cookie syncing:** A publisher's SSP could sync cookies with a DMP or DSP to allow advertisers to bid on impressions that will be shown to a user in their target audience.
2. **Deal IDs in PMP deals:** Private marketplace deals allow publishers to offer their most prized inventory to a select group of advertisers. By broadcasting their audience segments in PMP deals, publishers can earn even more money on their premium inventory.
3. **Segment ID in RTB auctions:** A publisher's SSP or DMP can pass segment IDs to DSPs during real-time bidding (RTB) auctions to help advertisers find their target audience.

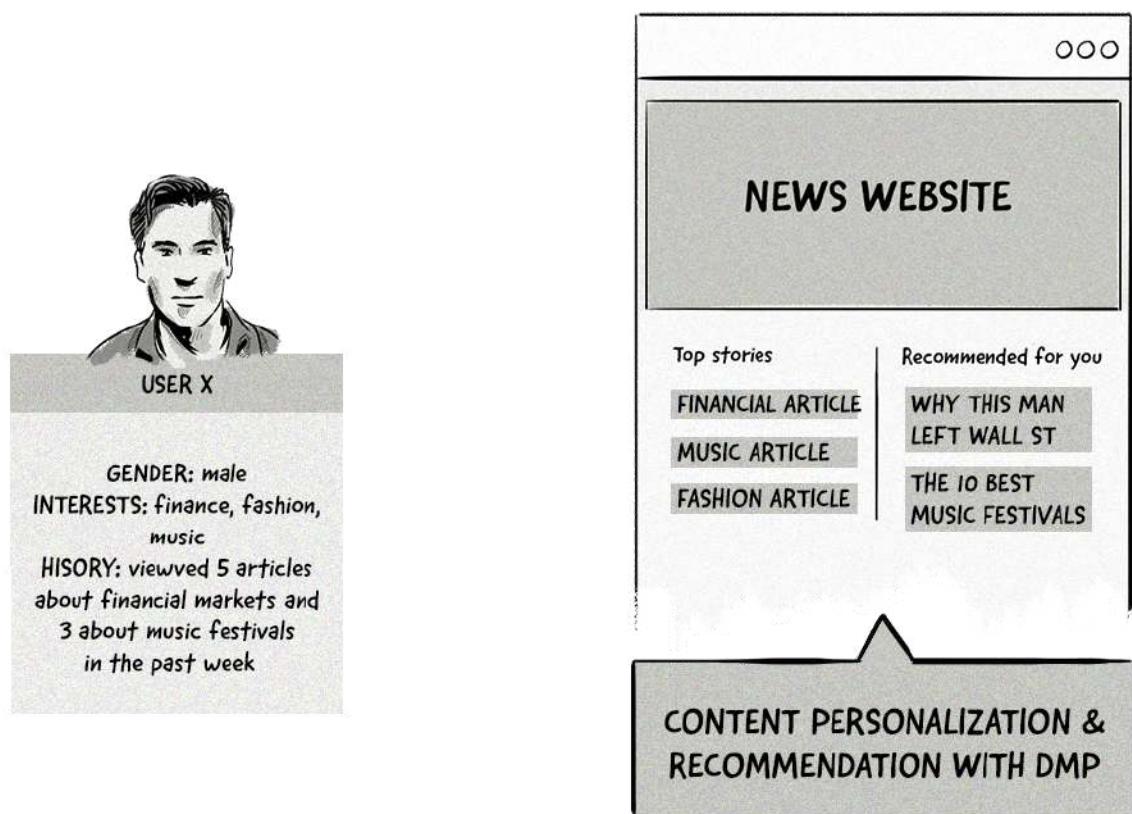
Improve Engagement and Conversions With Content Personalization

Content personalization involves displaying content and recommendations that match users' preferences based on their demographic information, interests, and the content they've consumed in the past.

The example below illustrates how using a DMP for content personalization works:



Content personalization on a site that doesn't use a DMP.



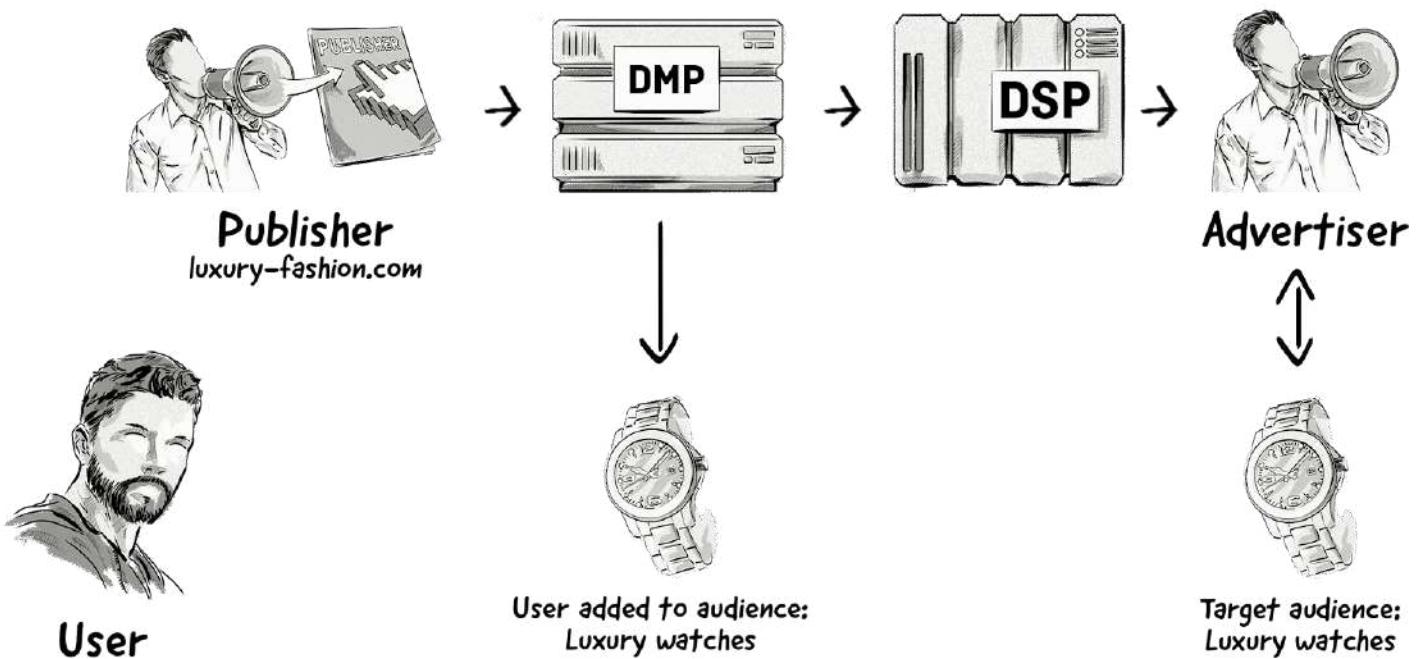
Content personalization on a site that does use a DMP.

Audience Extension For Publishers

Publishers can use a DMP to create audience segments, which can be used for audience extension.

Audience extension involves a publisher creating audiences from their first-party data, which includes contextual and behavioral data like age, location, interests, web history, purchase history, click-based interactions, etc.

Publishers can then push these audiences to AdTech platforms, allowing advertisers to target these audiences across the Internet — not just target them on the publisher's websites.



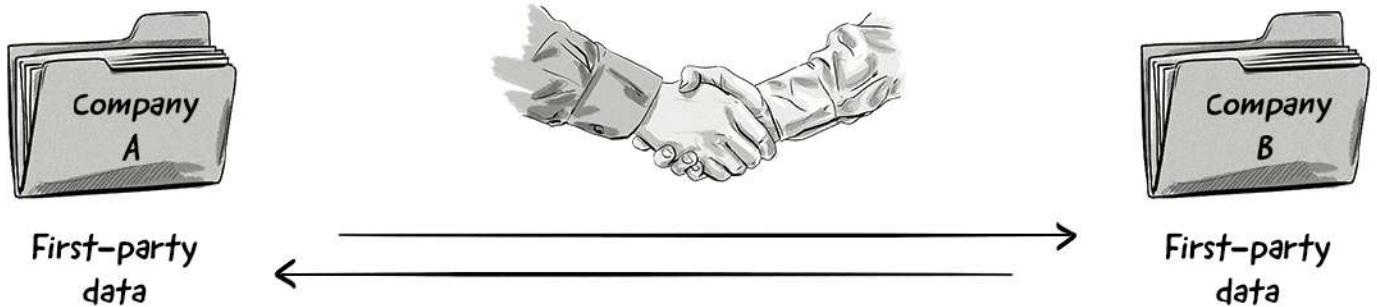
Here's an overview of how audience extension works:

1. The publisher's DMP collects its first-party data and creates audience segments.
2. The DMP passes on the publisher's audience segments to advertisers via DSPs. This is done via cookie syncing.
3. If an advertiser's DSP identifies a publisher's audience during an RTB auction originating from a different website, then it bids on that impression.
4. If the DSP wins, the ad is displayed to the publisher's audience but on a different site.

Audience extension is a win-win for publishers and advertisers — it allows publishers to create a new revenue stream and advertisers to find their target audiences across more websites.

Data Partnership

The publisher can set up a direct and exclusive partnership with another website, for example, a site that wants to run ad campaigns targeted at people living in the New York area that listen to the music online. The data used by the second website then becomes second-party data.



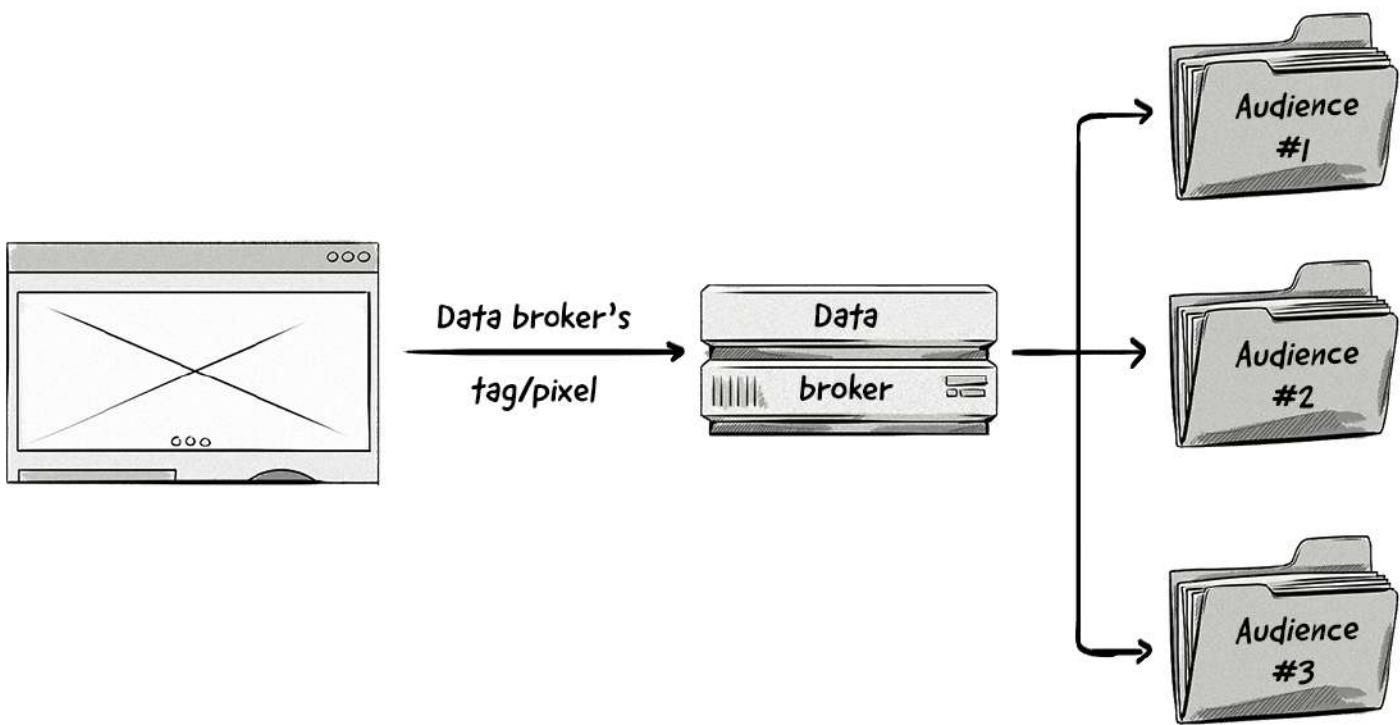
Data partnerships allow publishers to monetize their data.

Selling Their Data

The publisher could also just sell the segments or anonymized user profiles to data companies (e.g. data brokers and DMPs).

The data broker could either use the segments created by the publisher or group the anonymized user profiles into demographic segments based on different characteristics, such as location, age, interests, etc.

The data broker would then resell the data to advertisers who want to direct their campaigns to a specific demographic group. The data in these user segments would now be classified as third-party data.



Publishers can monetize their data via a data broker.

Compared to the partnership option, this monetization process is much less transparent. The publisher also loses its independence, as it is the data broker who decides which segments of data are shared and what kinds of segments are created from the publisher's visitors.

Data Brokers and Integrations With Programmatic Media-Buying Platforms

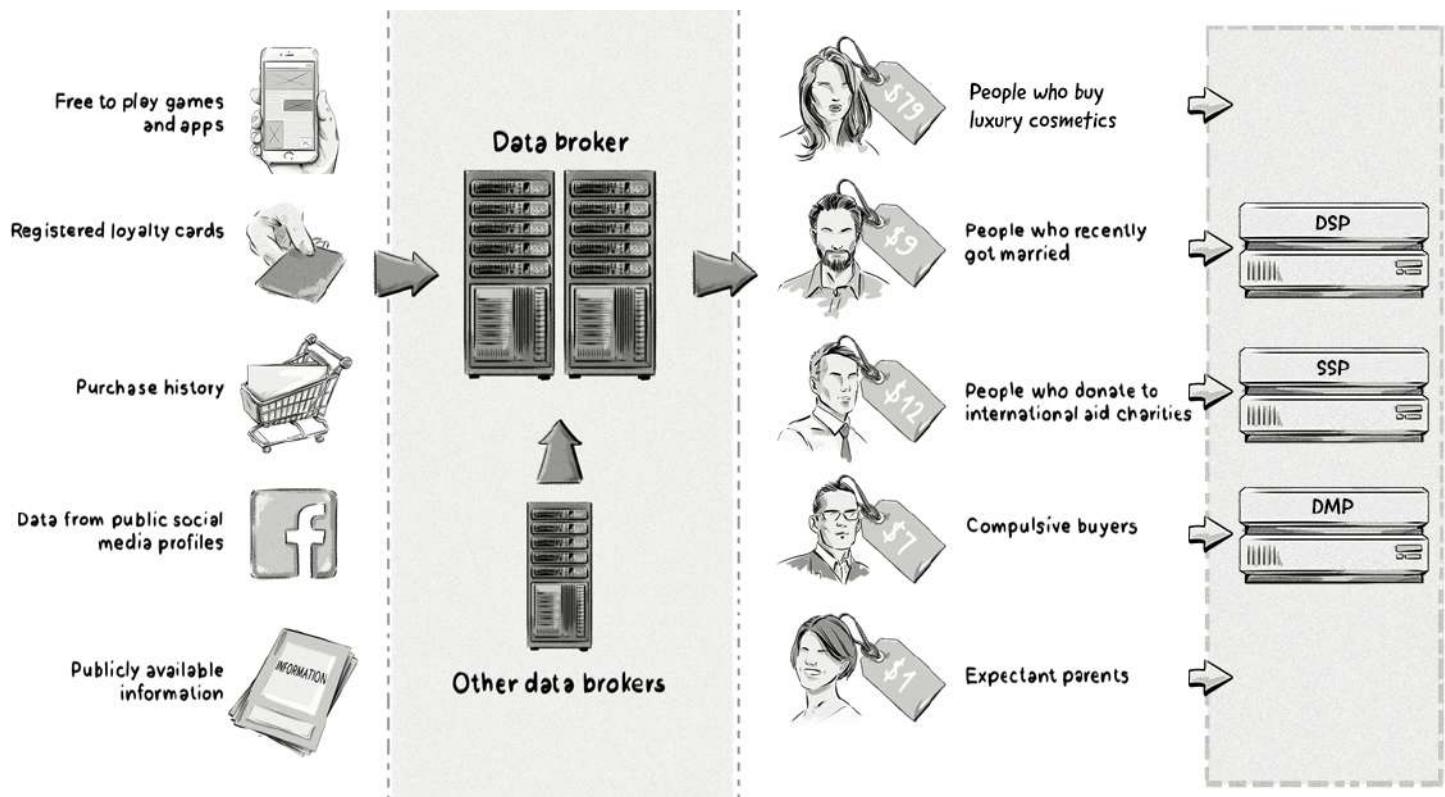
While all companies that operate within the online advertising industry collect data, there are some companies that make a business only out of collecting and selling online consumer data. These companies are known as **data brokers**, or **information brokers**.

What Is A Data Broker?

A data broker is a company that aggregates user profiles from publishers and brands, combines them together, segments them, and then sells the segments to other companies to use in their online advertising campaigns.

There are several types of data brokers that operate in certain industries:

- **Marketing and advertising:** Improve ad targeting and campaign measurement.
- **Identity verification and fraud detection:** Help organizations like banks verify the identity of individuals.
- **People search:** Collect publicly available information about people from social media websites.



DMPs and data brokers collect data from various sources, create audiences, and then sell them to AdTech companies.

Some examples of data brokers in online advertising include:



In the digital advertising and marketing industries, many DMPs act as data brokers and vice versa. The data collection process is similar to that of DMPs (listed above).

Data Pricing Models

Once DMPs and data brokers have collected the data, they usually sell it on to advertisers and AdTech vendors via two pricing models: **a fixed CPM or a percentage of the media cost.**

Fixed CPM Price

The most common way for DMPs and data brokers to sell data is on a cost per mille (cost per thousand) basis.

This means they are paid a fixed amount, such as \$1.25 for each 1,000 unique cookies created by their site(s).

The main advantage of this model is that it provides a guaranteed price for both the data provider and advertiser/media buyer.

However, it doesn't take into account important variables, such as context or the real value of the ad placement, meaning it places a fixed price on the audience which could actually be worth more than the CPM price suggests.

There are also issues surrounding the ROI of audience data sold on a fixed CPM price.

Often, the CPM price of audience data is actually more than the CPM price of the impression itself. This means that an advertiser could buy an impression on a CPM of \$1.10 but the CPM of the audience data could be \$1.25, which adds significant cost and makes generating a reasonable ROI much harder to achieve.

Percentage of the Media Cost

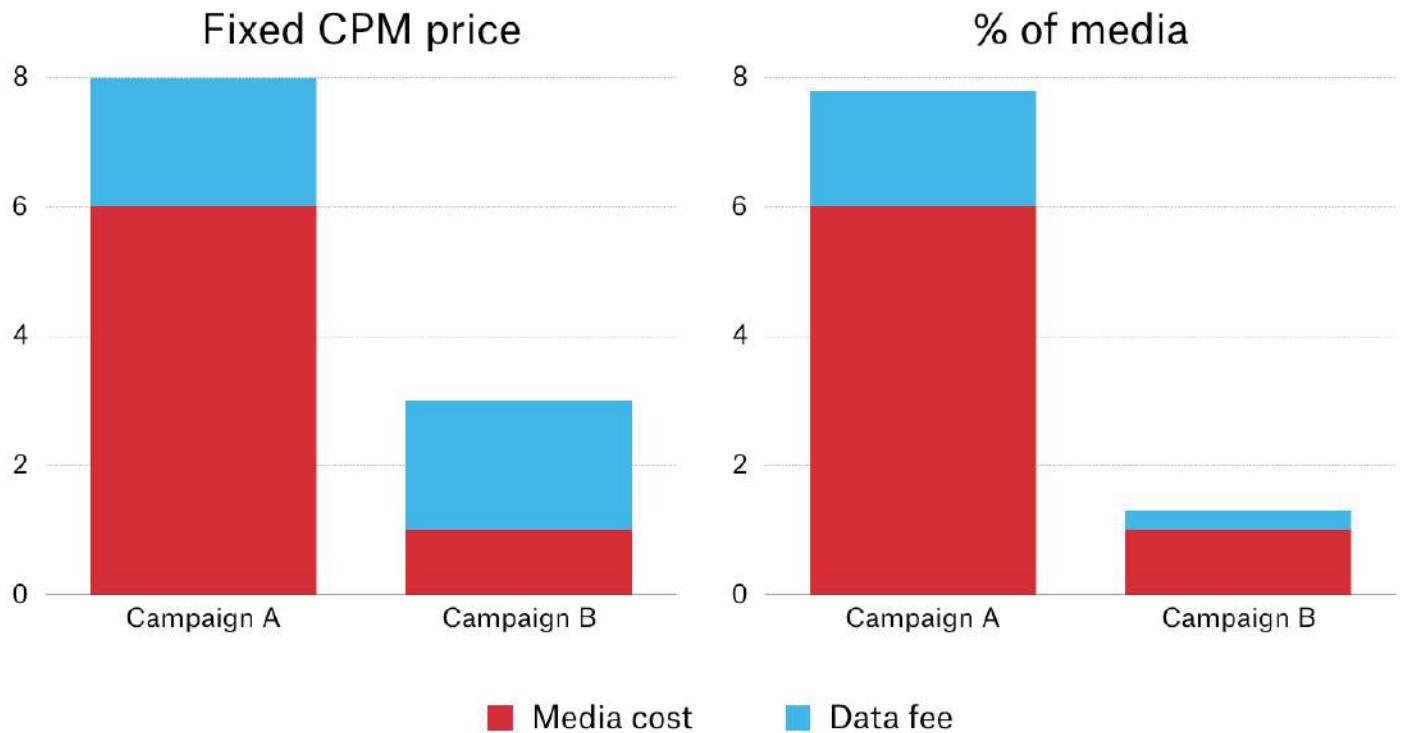
Many data brokers and advertisers/media buyers are moving towards a percentage of media cost pricing model due to the very issues the fixed CPM pricing model presents.

As the name suggests, data providers charge advertisers and media buyers a percentage of the media cost for their audience data.

So if the impression was sold at a CPM of \$.50 and the data provider charged 20% of the media cost, then the advertiser or media buyer would pay \$.10 for the audience data.

While it may appear that the data brokers is losing money via the % of media cost, they are actually making third-party data more valuable and useful for advertisers and media buyers as they benefit from improved targeting, optimized ROIs, and better campaign performance — all of which lead to high adoption rates of third-party data, which spells good news for data brokers.

The image below illustrates the cost differences associated with the **fixed CPM pricing model** and the **% of media cost pricing model:**



The % of the media cost pricing model is a fairer and more accurate way of selling third-party data to advertisers and media buyers.

Some common problems with using third-party data in programmatic media buying:

Problem 1: The main issue with this method of selling through technology platforms is that it's often hard to know whether a DSP used a certain audience from a DMP.

In the RTB auction model, data is usually provided in every bid request sent to the DSP. The bidder on DSP side sends bids on behalf of the advertiser, but there is no way to tell if the bidder used the data during the exchange.

Problem 2: The other problem with this model is that the price of the data is usually static.

The only difference is that some segments are considered premium or of higher value than others, and the CPM price is then higher. There is no way to dynamically set the price for the data based on the demand and/or quality, and therefore, all the parties in the ecosystem (e.g. publishers, data suppliers, data providers, advertisers, etc.) may be losing out financially.

The Future of DMPs

Because every digital advertising process is powered by data, DMPs have been a key component of a brand's, agency's, and publisher's tech stack.

But the business model and future of many DMPs is in jeopardy because of the rise of privacy in AdTech.

Privacy laws like the GDPR, ad blockers, and privacy settings in web browsers are making it much harder to collect third-party data from websites.

Google Chrome's announcement that they'll be shutting off support for third-party cookies by 2022 (rough timeline), means that almost 100% of web browser traffic won't support third-party cookies.

To survive the next decade, most DMPs will need to look for ways to help publishers and advertisers identify their audiences without the use of third-party cookies, for example, by using identity resolution services.

Advertisers and publishers will also need to think about how they unlock the value of their first-party data.

In fact, this is already happening with the rise of **customer data platforms (CDPs)**.

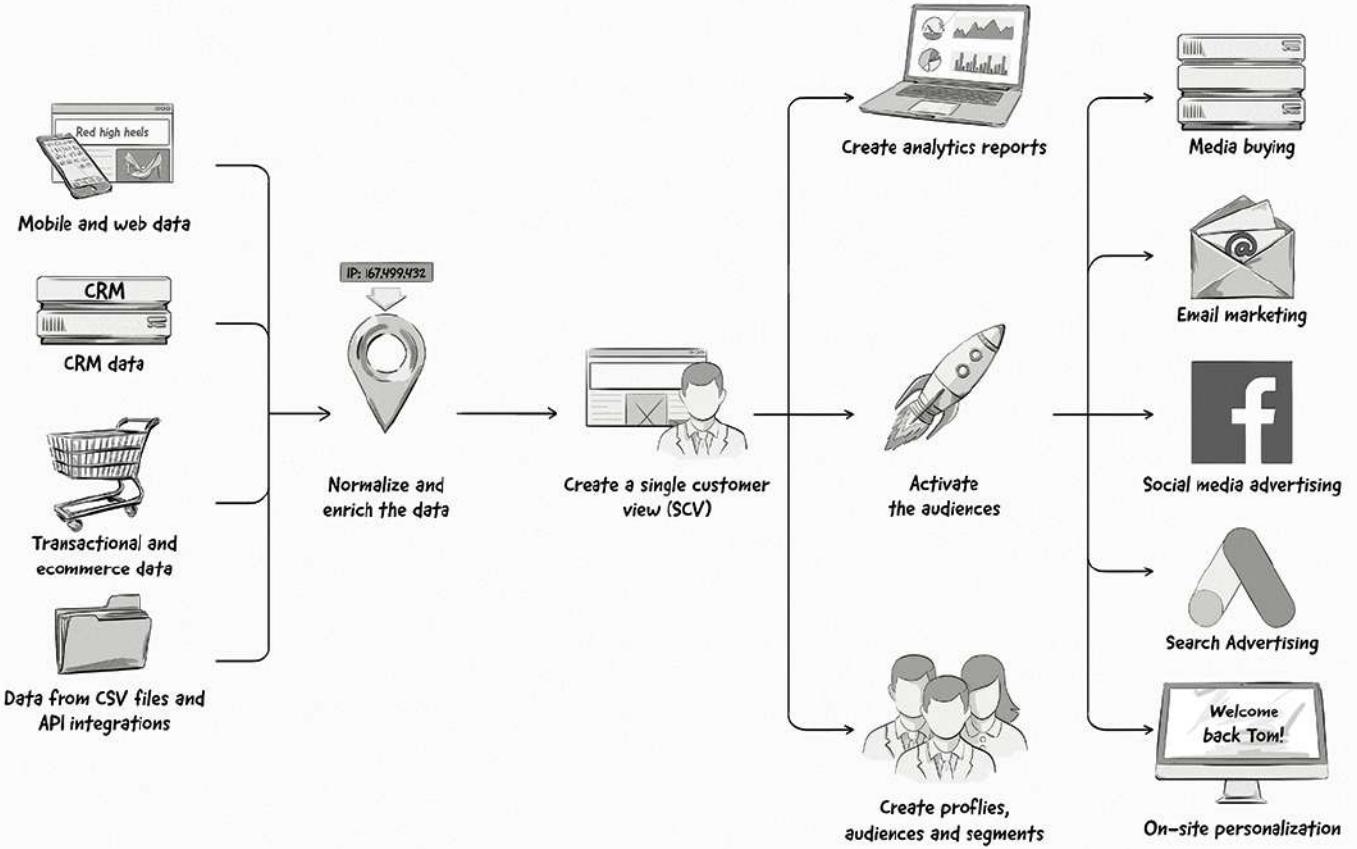
What Is a Customer Data Platform (CDP)?

A customer data platform is a piece of software that collects data from different sources and creates a single customer view of a customer, aka single customer view (SCV).

Although DMPs and CDPs are fairly similar in the way they collect, normalize, enrich, and activate data, there are a couple of main differences in the type of data they collect and how they use it.

As we mentioned above, DMPs typically collect third-party data and use it for advertising purposes. CDPs mainly collect first-party data and use it for multiple purposes, such as advertising, marketing, and customer support.

The anatomy of CDP



The image above illustrates how CDPs work and common advertising and marketing use cases.

The rise of privacy laws and changes to web cookies has forced advertisers and publishers to put more focus on utilizing their first-party data.

Publishers, for example, can collect first-party data, create user profiles and audiences in a CDP, and offer those audiences to advertisers for ad targeting.

Now that we've had a detailed look at the role data plays in the online advertising ecosystem, it's time to turn our attention to an area that heavily relies on data - **attribution**.

12. Attribution



Identifying users across online channels, online and offline channels, and across numerous devices is a critical part of digital advertising as it allows advertisers to gain a better understanding of how their audience interacts with their brand and improve the customer journey.

But more importantly, it allows them to attribute conversions and goals.

What Is Attribution?

Attribution is the process of identifying which touchpoints a consumer interacted with or was exposed to during a period of time before they completed a goal set by an advertiser or marketer. Attribution allows advertisers

and marketers to make improvements to their campaigns by understanding which touchpoints are working and which ones aren't.

Attribution has always been a part of advertising and marketing, even before the Internet, but it's through the use of data and technology that advertisers and marketers of today are able to more accurately attribute conversions.

In this chapter, we cover the methods used to identify and track users as they move through the offline and online worlds and across different devices, and look at the various techniques used to attribute conversions.

To learn about how conversions are recorded, read chapter [08. Tracking and Reporting Impressions, Clicks, and Conversions in AdTech Platforms](#).

What is a customer journey?

A customer (aka user) journey is the path a person takes from the time they first become aware of a brand to the time they complete a goal defined by an advertiser or marketer (e.g. a purchase or download).

Although everyone will have a different customer journey, it's useful for advertisers and marketers to understand how the different stages of a customer journey and the interactions a person has influence their decision to complete a goal.

Each interaction a person has with a brand during their customer journey is known as a touchpoint.

What is a touchpoint?

A touchpoint is an interaction a user has with your brand on different channels.

But a user doesn't have to actually interact with the touchpoint for it to count. For example, if a user sees a display ad from a brand but doesn't click on it, then it's still classed as a touchpoint.

Examples of touchpoints include:

- Website visits
- Product views
- Reviews
- Blog posts
- Ebooks and whitepapers
- Digital ads
- Social media content
- Videos
- Emails
- Store visits

In many cases, these touchpoints will influence a person's perception about your brand.

Advertisers and marketers will tailor the messaging across different touchpoints depending on where the person is in the customer journey (e.g. awareness, consideration, and purchase).

For example, advertisers and marketers could run display ads to make people aware of their product. They could then run retargeting ad campaigns on Facebook targeting people who have visited their website to encourage them to make a purchase.

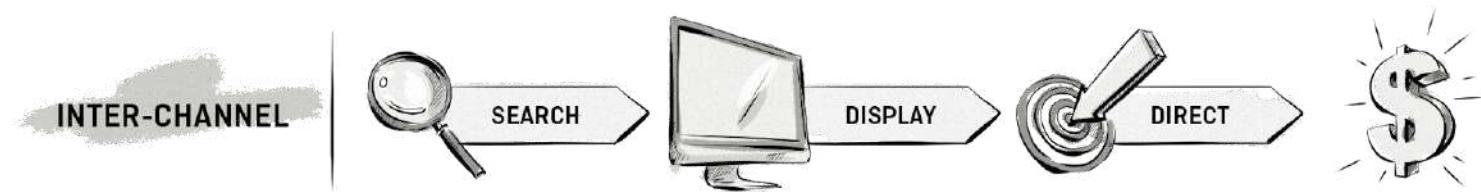
We'll now look at the different types of attribution.

Online to Online Attribution Models

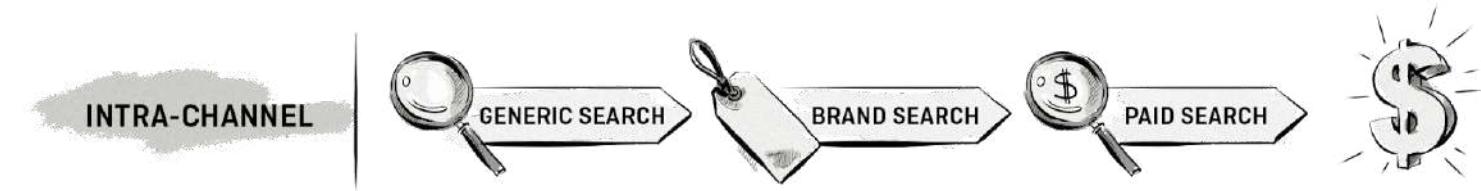
Online to online attribution identifies which touchpoints a user had before they completed a goal across different online channels.

As the goal of most online ad campaigns is to drive users to a website, advertisers and marketers view attribution reports provided by web analytics tools, MarTech platforms like marketing automation platforms and attribution software, and AdTech platforms like ad servers.

There are two main types of online to online attribution — **inter-channel** and **intra-channel**.



Inter-channel attribution looks at touchpoints across different channels.



Intra-channel attribution looks at touchpoints in the same channel.

How Does Online Attribution work?

When it comes to detecting which online channels and interactions a user had in their customer journey, there are a few ways you can do this.

The simplest way is to use the Referrer field in the HTTP protocol when a user is directed from an online channel to your website.

The Referrer field is passed with every request from the browser to the web server. Here's an example of a standard HTTP GET request:

```
GET / HTTP/1.1
Host: clearcode.cc
DNT: 1
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Referrer: http://publisher1.com/article-about-adtech.html
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8
(KHTML, like Gecko) Version/10.1.2 Safari/603.3.8
...
```

In this example, a user was reading an article on publisher1.com and then clicked on a link (or ad) and was directed to <https://clearcode.cc>.

Web analytics tools, and AdTech and MarTech platforms will display the following referrers:

Direct

When a visit is marked as direct it means that the referrer information isn't known.

There are many reasons why a referrer can be marked as direct:

- The user entered the URL in their browser's web address bar or accessed it from their bookmarks.
- The user entered the website from a subdomain, e.g. they first accessed publisher1.com and then clicked on a link that took them to blog.publisher1.com.
- The user clicked on a link or ad in a native mobile app that didn't contain UTM parameters in the URL (e.g. publisher1.com/?utm_campaign=native-app).
- There were some technical issues that resulted in referrer loss, such as clicking on a link from a secure website (<https://>) to an unsecure website (<http://>). The table below illustrates when referrer loss occurs between secure and unsecure websites:

HTTP protocol	Referrer passed or lost?
https:// to http://	Referrer lost
http:// to https://	Referrer passed
http:// to http://	Referrer passed
https:// to https://	Referrer passed

As most websites nowadays use the secure <https://> protocol, this is less of an issue.

Organic

Organic traffic comes from a search engine like Google Search, Bing, and DuckDuckGo.

If an advertiser or marketer is running paid search ads, then these would be marked as ‘campaign’ (see below).

Social

Visits from social media sites like Facebook, LinkedIn, Twitter, and YouTube are marked as ‘social’.

Website

When a user clicks on a link from a website and is directed to the advertiser’s website, then it’s classed as a ‘website’ referrer (like in the example above).

Campaign

The ‘campaign’ referrer is recorded when the website a user lands on contains UTM parameters. In this case, the Referrer field is ignored and the UTM parameters are used to determine the referrer.

Some AdTech and MarTech platforms will just list this referrer as ‘Campaign’, while others will mark them as ‘Paid social’ or ‘Paid search’, depending on what information is contained in the UTM parameters.

For example, if a user clicks on a LinkedIn ad and is directed to a website containing the UTM parameters below, then the referrer could either be recorded as ‘Campaign’ or ‘Paid social’.

```
?utm_source=linkedin&utm_medium=ad&utm_campaign=linkedin-ad
```

Similarly, if a user clicks on a paid search ad on Google and is directed to a website containing the below UTM parameters, then the referrer could either be recorded as ‘Campaign’ or ‘Paid search’.

```
?utm_source=google&utm_medium=ad&utm_campaign=paid-search-ad
```

Every time the user comes from a different channel, a new session (visit) starts and the referrer information is recorded, which helps paint a picture of the user journey.

Online Attribution Models

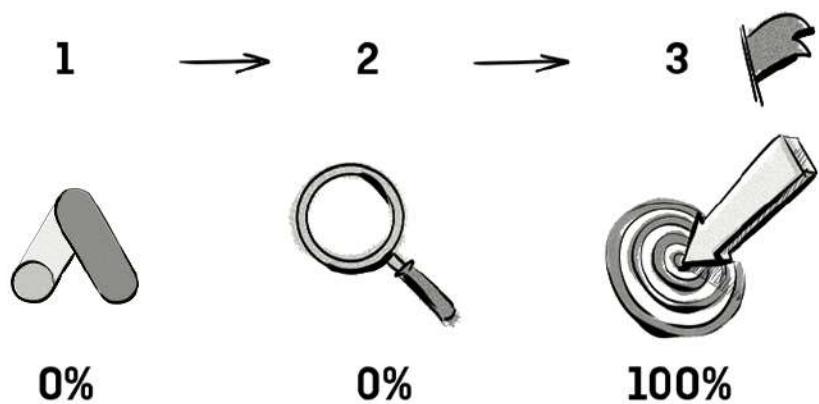
Now that we know how the different online channels are detected, we’ll now look at the different online attribution models.

1. The Last Click Attribution Model

The **last click (aka last interaction or last touchpoint) attribution model** is the oldest model out of them all and despite the number of new attribution models, it is still the default model in many web analytics, MarTech, and AdTech platforms.

The last click attribution model assigns 100% of a conversion to the last known referral, click, or traffic source.

So if the last action before a conversion was a direct entry, then 100% of the conversion would be attributed to the direct entry.



Although this model is one of the simplest, it ignores all the other touchpoints in a customer journey, which can lead to poor decision making when choosing which channels to optimize.

2. The Last Non-Direct Attribution Model

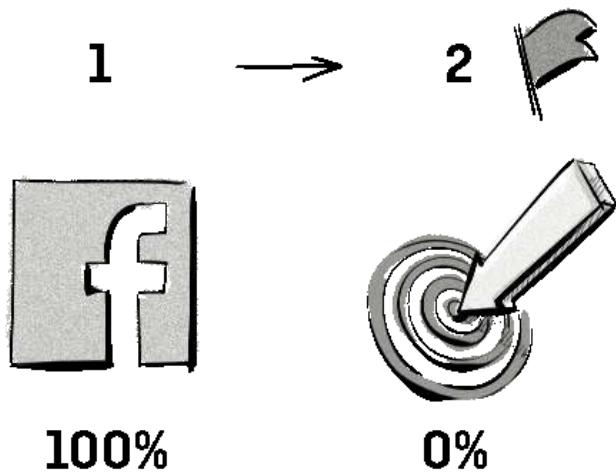
The **last non-direct** attribution model is very similar to the last click attribution model but it removes direct visits from the equation.

With this model, 100% of a conversion is attributed to the last known referral that *wasn't* a direct visit.

Here's an example of how this process looks:

1. A user clicks on a link on Facebook and is directed to your website.
2. They browse your website but then leave.
3. They later type your website into their address bar and download one of your ebooks.

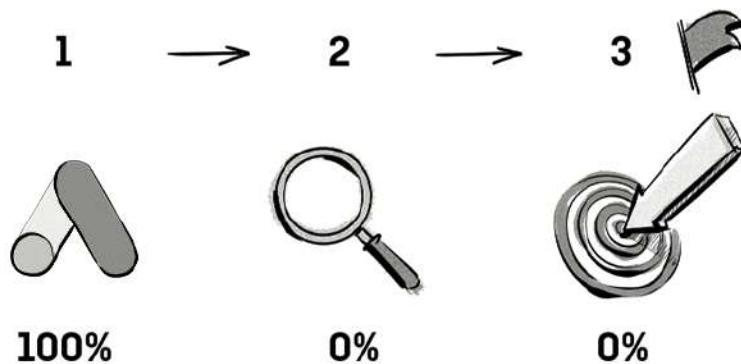
Because the third step is a direct visit, the last non-direct attribution model would ignore this and assign 100% of the conversion to Facebook.



This model is better than the last click model, but still doesn't take into account the other touchpoints a person has in their customer journey and can also lead to bad decisions.

3. The First Click Attribution Model

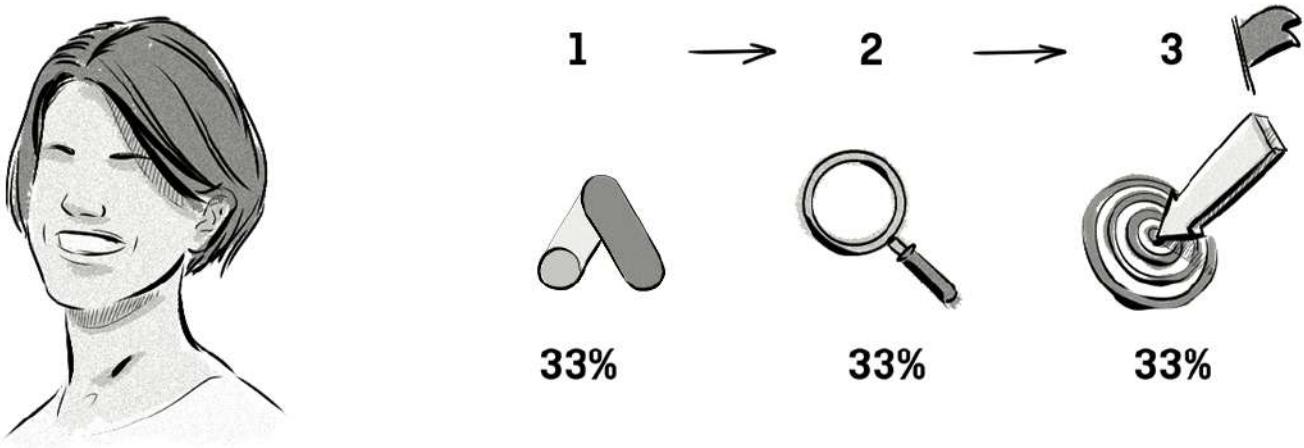
The **first click (aka first interaction or first touch) attribution model** is similar to the previous two, except it assigns 100% of a conversion to the first click or referrer in the customer journey.



This model suffers from the same drawbacks as last click and last non-direct attribution models.

4. The Linear Attribution Model

The **linear attribution** model evenly attributes conversions to all touchpoints in a customer journey.



Even though this model values each conversion equally, which rarely is the case, it is useful for getting an overview of the customer journey.

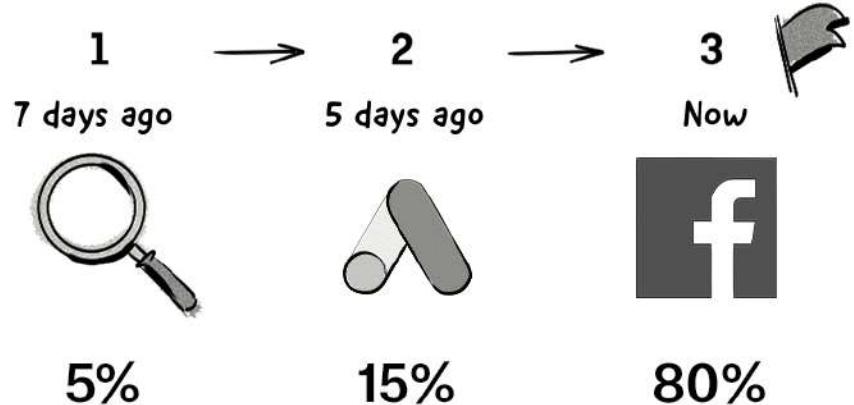
5. The Time Decay Attribution Model

The **time decay** attribution model is a modification of the linear model.

With this attribution model, the touchpoint that is closest in time to the conversion gets the most credit.

The remaining touchpoints are given credit based on how far away they are from the conversion. Put simply, the further away a touchpoint is from a conversion, the more its credit “decays”.

It not only provides the full picture of the customer journey but also assigns a certain weight to each touchpoint based on the time difference between each touchpoint.



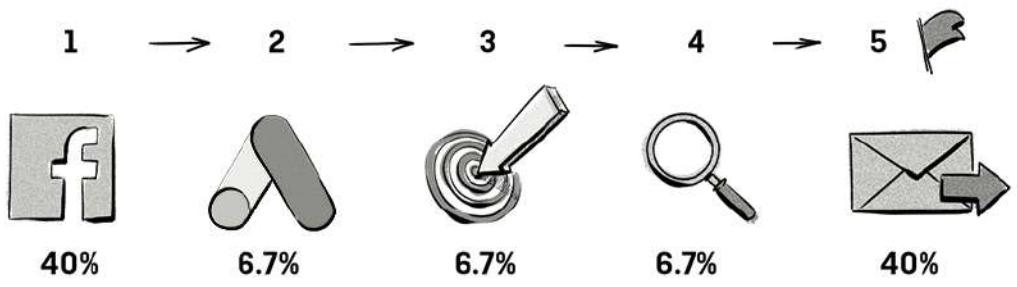
The above image illustrates how the different touchpoint could be attributed for the conversion.

This model assumes that the most recent touchpoints were the ones that influenced the user to convert, which may or may not be the case.

6. The Position Based Attribution Model

The **position based attribution model** grabs all the touchpoints in the customer journey and assigns them credit based on their position in the conversion path.

This model gives more weight to the first and last interaction in the customer journey. The rest of the attribution credit is divided among the remaining touchpoints.



This model is often a good choice for advertisers as it provides an overview of the customer journey and assigns credit to the two most important interactions — the first and last interactions.

7. The Custom Attribution Model

Some AdTech and MarTech platforms allow you to create custom attribution models whereby advertisers set their own rules for attributing touchpoints in a customer journey.

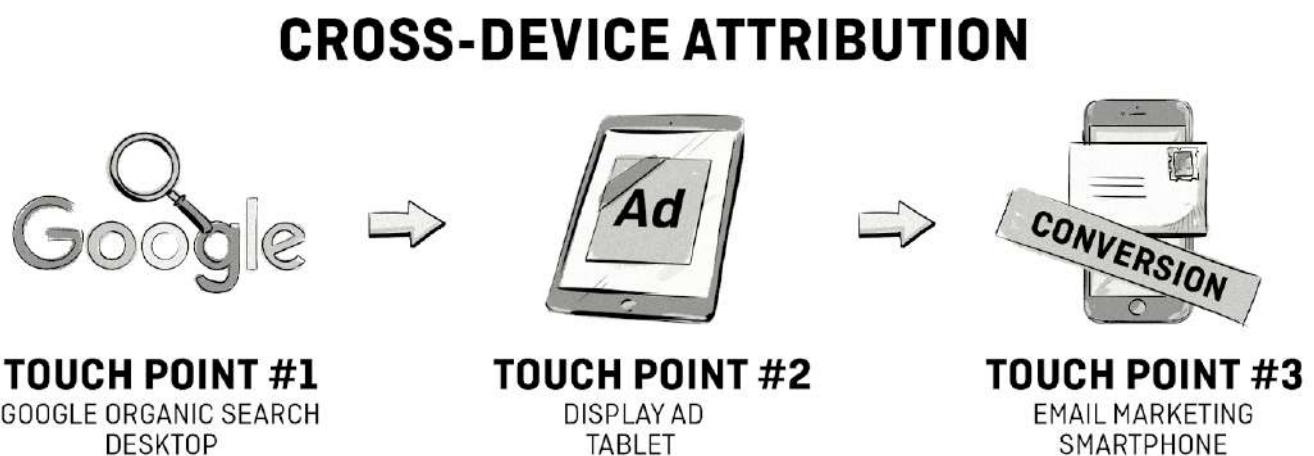
This option is often a good choice for advertisers as they can take into consideration the specifics of their campaigns, their customers, and customer journey.

The above online attribution models are specific to one device (e.g. a laptop and smartphone) and web browser (e.g. Safari, Firefox, and Google Chrome). If we want to attribute conversions from different devices and web browsers, then we'll have to use cross-device attribution.

Cross-Device Attribution

Cross-device attribution aims to record interactions a user has with a brand across multiple touchpoints and devices, and ultimately attribute conversions accordingly. Where online attribution models aim to attribute conversions across different channels, multi-touch attribution aims to attribute conversions across different web browsers and devices, as well as channels.

Here's an example of how cross-device attribution would look:



How Does Cross-Device Attribution Work?

To attribute online conversions between different channels, AdTech and MarTech companies use cookies — typically third-party cookies.

However, because cookies are tied to one device and one web browser, they can't be exported to another, meaning they are useless for cross-device attribution.

To attribute conversions across different web browsers and devices, measurement companies use deterministic matching, probabilistic matching, or a combination of both.

We explained what these two methods are and how they work in a previous chapter (10. User Identification), but here's a recap:

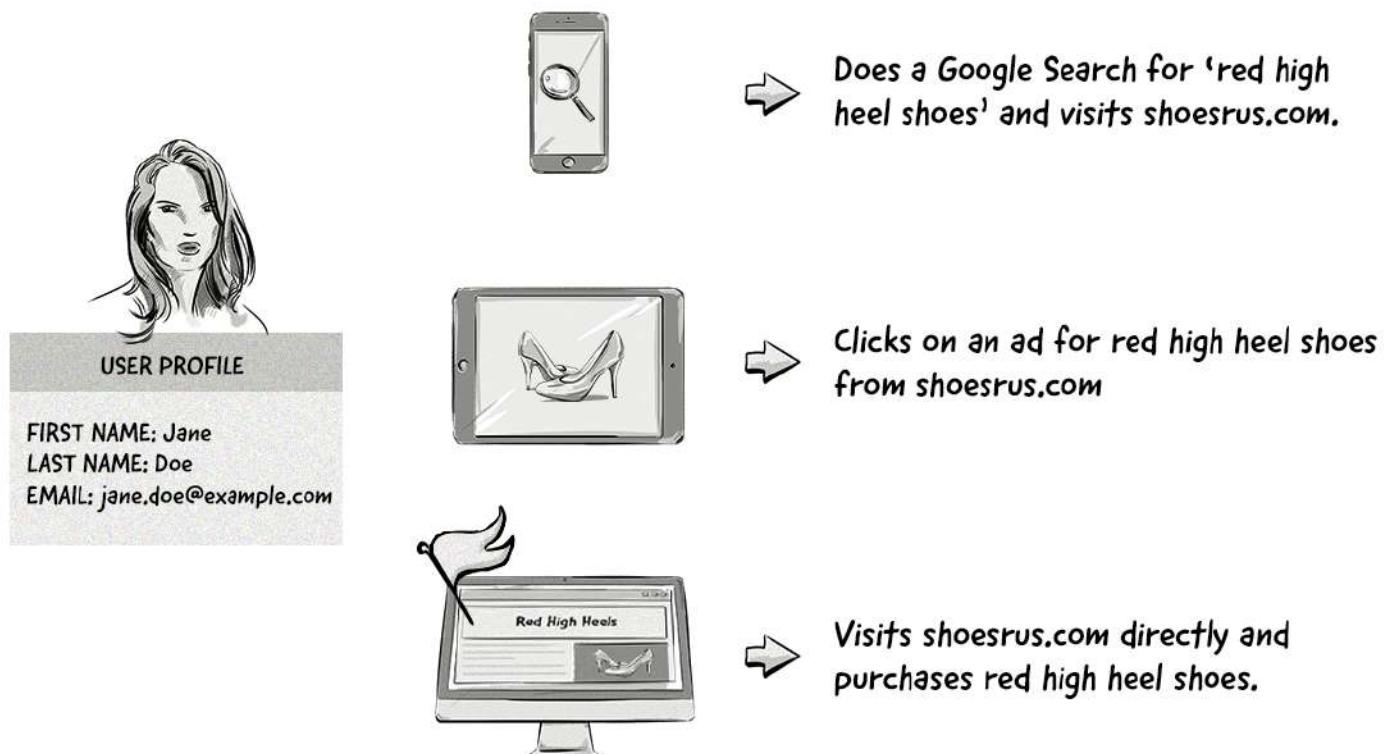
Deterministic matching uses common identifiers, such as email addresses and phone numbers, to identify and match users across different devices.

Probabilistic matching uses less-common pieces of data, such as IP addresses and location data, to identify and match users across devices. Because the data isn't as accurate or unique as deterministic data, probabilistic matching also uses algorithms and statistical modeling to make a match.

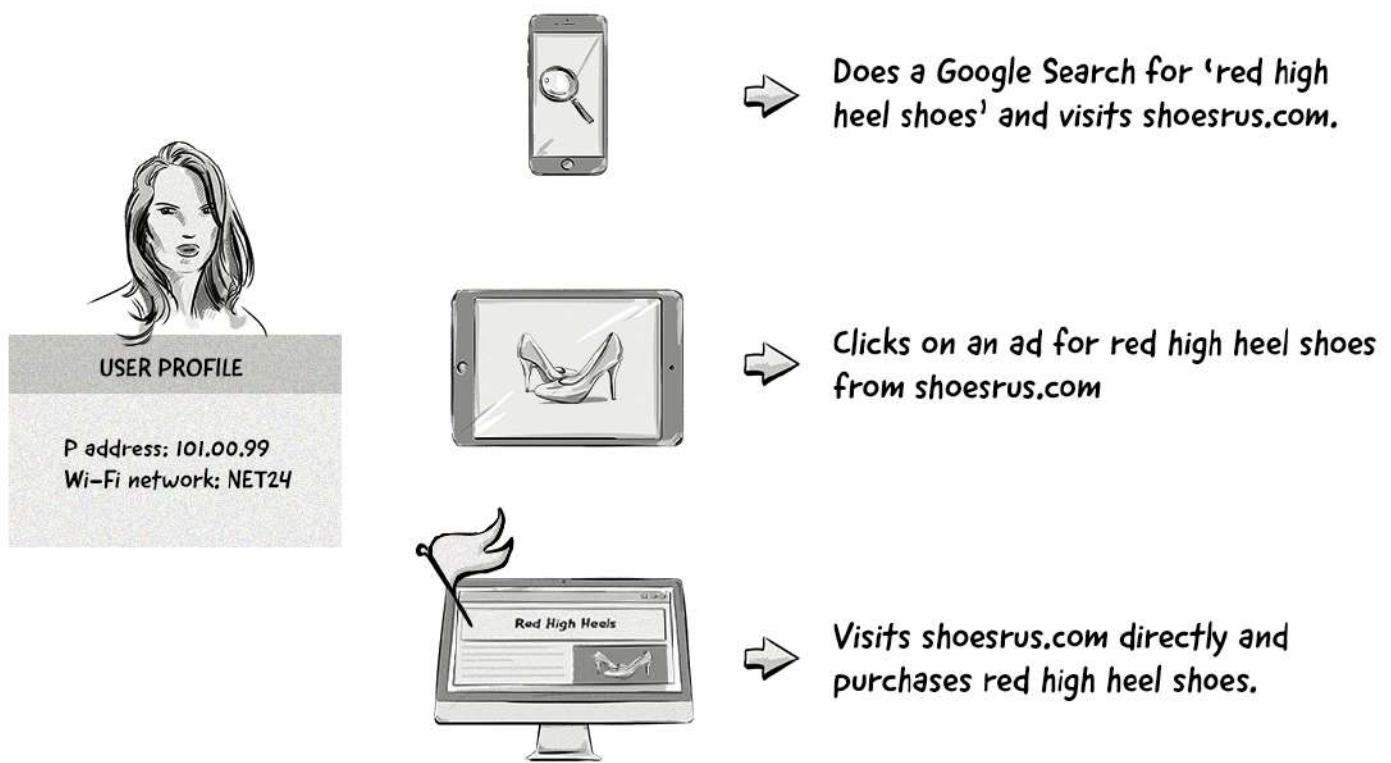
To use these methods for cross-device attribution, AdTech and MarTech companies would create user profiles that collect and contain these pieces of data.

Below are two examples of how deterministic matching and probabilistic matching can be used for cross-device attribution:

Deterministic matching for cross-device attribution



Probabilistic matching for cross-device attribution:



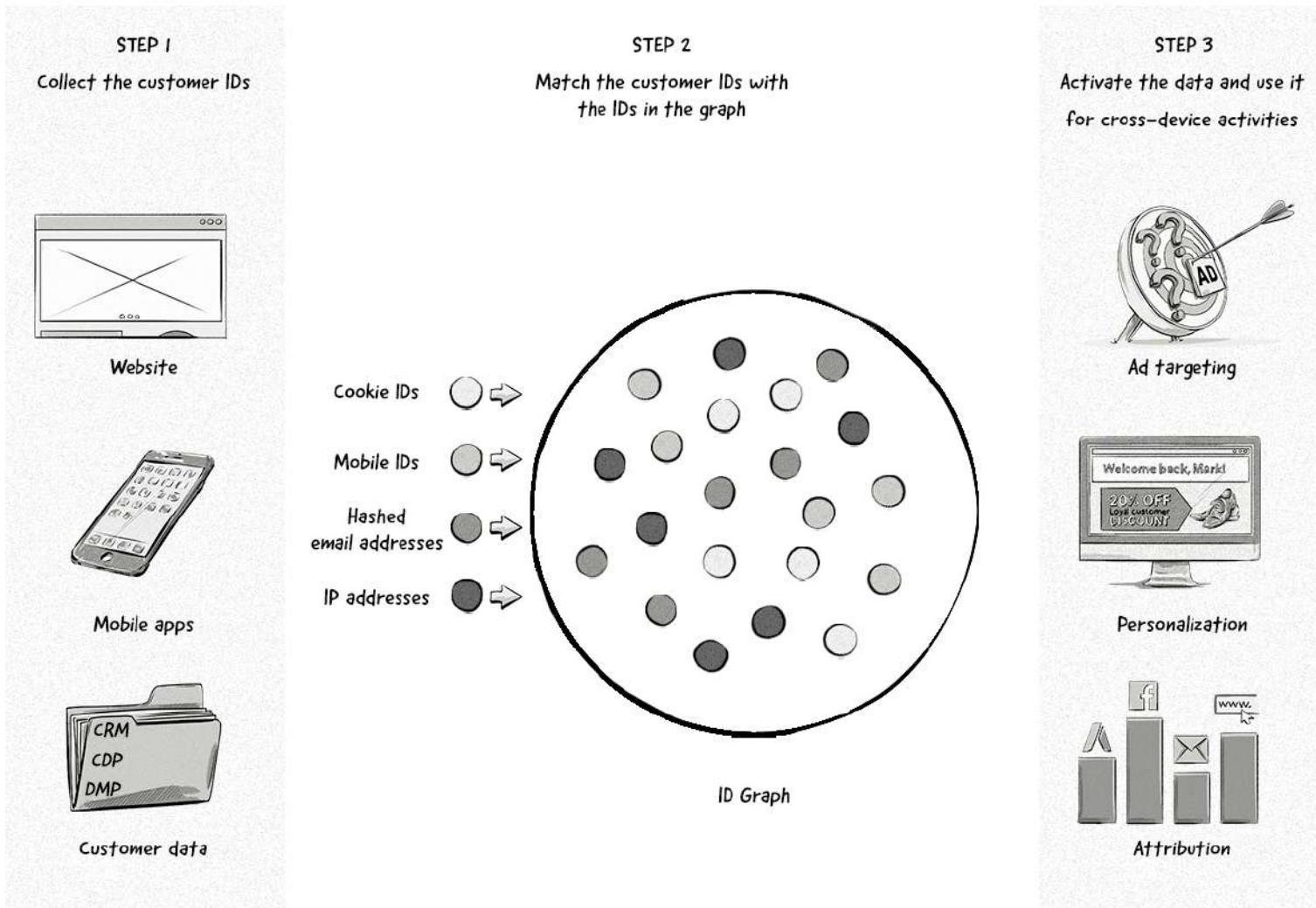
As we can see in the examples above, the actual attribution process is similar for both deterministic and probabilistic matching. The main difference is the data that is used to identify the user and attribute the conversion.

For walled gardens like Google and Facebook, attributing conversions with deterministic matching is much easier than for independent AdTech companies because of the types of data they collect — e.g. email addresses and names — and because many users will use their Facebook or Google account across different devices.

If brands, agencies, and independent AdTech companies (e.g. DSPs) want to conduct cross-device attribution, then they'll need to use a DMP like [LiveRamp](#) or a cross-device measure platform like [Tapad](#).

These companies will collect user data from different online and offline sources, create user profiles, and produce a graph — sometimes referred to as an identity, ID, or device graph. Brands, agencies, and tech companies then use these graphs for identification, ad targeting, and attribution.

How ID Graphs Work



An illustration of how ID graphs work.

Learn more about the various identity solutions and how they work in chapter 10. **User Identification**.

Offline-Online Attribution

Even though advertising and marketing is moving online, there is still a need to combine the offline data with online data and attribute and track users across offline and online sources.

For example, it's important for advertisers to know whether a billboard ad resulted in a website visit or online conversion.

Examples of offline channels include:

- Direct mail
- Traditional outdoor advertising — i.e. out-of-home (OOH) and digital out-of-home (DOOH) advertising.
- Telemarketing

- TV
- Radio

Below are the most common ways for advertisers to attribute offline ad exposure with online conversions.

Vanity URLs

Vanity URLs are domain names that are often created for a specific advertising campaign. They're designed to match the company's brand, be easy to remember, and shorter than the actual URL of the landing page. Companies use vanity URLs to promote a new product or service and use them in OOH, TV, and radio ads.

For example, instead of using a URL like

company1.com/new-product?utm_source=ooh&utm_medium=billboard-airport&utm_campaign=new-product, an advertiser could use newproduct.com.

The vanity URL could take the user to a dedicated landing page, (e.g. newproduct.com) or redirect them to a different landing page (e.g. company1.com/new-product). With either option, the vanity URL will redirect the user to a destination page and add campaign tracking parameters for traffic attribution.

There are different types of vanity URL:

1. Standalone vanity URLs, e.g. newproduct.com
2. Subpage vanity URLs, e.g. company1.com/newproduct
3. Shortened vanity URLs, e.g. sv.ly/newproduct

Vanity URLs are useful for measuring the reach and impact of offline ad campaigns and attributing them to online website visits and conversions, but they are not 100% accurate because some users who saw the ad may later perform a Google search for the product or service instead of typing in the vanity URL. This means any conversion that occurs as a result of this will be attributed to Google Search and not the offline ad.

However, it's still a valuable method for gauging the effectiveness of an offline ad.

Time-limited attribution windows

Another way to measure offline ad exposure to online web traffic and conversions is via the time-limited attribution window.

This model analyzes a period of time (e.g. 30 minutes) after the air time of a TV or radio advertisement and looks for increases in web traffic and conversions.

When applying this model, advertisers need to consider the following:

- How long should the window be open? E.g. should we look at web traffic and conversions 30 minutes after our radio ad aired or longer?
- How can we separate the traffic and conversions that were exposed to the campaign from the ones that weren't?
- How do we determine whether other campaigns influenced the increase in traffic and conversions during the attribution window?

Most AdTech and MarTech companies offer an attribution window model as part of their measurement offering, but it's often limited to one channel (e.g. display). If advertisers want to measure offline ad exposure to online web traffic and conversions, then advertisers will need to set this up manually in their analytics software or use a dedicated attribution tool.

Online surveys

Instead of using complex attribution models, advertisers could simply ask users how they found their website.

Although this is a very simple approach, it can provide valuable insights that you might not get with attribution models.

Advertisers can implement online surveys at three different levels:

- When a user fills out the purchase or sign-up form or on the confirmation page.
- When a user is browsing your website, open a discreet sidebar pop-up asking them to fill out a survey (you could offer a coupon code as an incentive).
- When the user is leaving the website, open a pop-up survey.

Thanks for contacting us!

We've just emailed you with a link to set up a call.

Before you go, we have a question for you...

How did you first hear about us?

Please select one of the options below

- Google Search
- LinkedIn
- Someone told me about you
- Twitter
- Quora
- Other websites
- Other

SUBMIT

Even though not every user will fill out a survey or just select a random field, advertisers will still have enough data to compare the survey results with their attribution and traffic source data.

Coupons

Coupons have been around for decades but their popularity and effectiveness for attributing conversions is still strong.

By using coupons in their marketing materials, advertisers can attribute conversions to specific offline channels, often with more accuracy than with attribution models and technology platforms.

Coupons work best with direct mail campaigns and other printed advertising materials, but it's a good idea to issue unique coupons per campaign, and when possible, per client.

Zip/Postal codes

Collecting zip codes from online customers can be used to measure different offline campaigns, such as direct mail and out-of-home campaigns.

Although this method won't be very accurate — you won't know for certain whether someone with a certain zip code was influenced by your campaign — it can be used in conjunction with the models listed above for improved accuracy.

This approach would really only make sense for ecommerce stores, or companies that have an offline and online store, as they collect billing and delivery information during the purchase process.

Online-Offline Attribution

Let's now look at a few ways advertisers can attribute online activity, such as ad views and clicks, to offline purchases in a store.

Beacons

Beacons are bluetooth-enabled devices that can transmit signals to and from mobile devices such as smartphones and tablets.

When placed in brick-and-mortar stores, they can be used to send push notifications to devices in a certain radius and collect data about the device itself. The latter can help attribute online activity, such as ad clicks and mobile app activity, to offline purchases.

Zip/postal codes at POS

You read a moment ago about how advertisers can use zip codes to attribute offline ads to online conversions, but they can also be used in reverse.

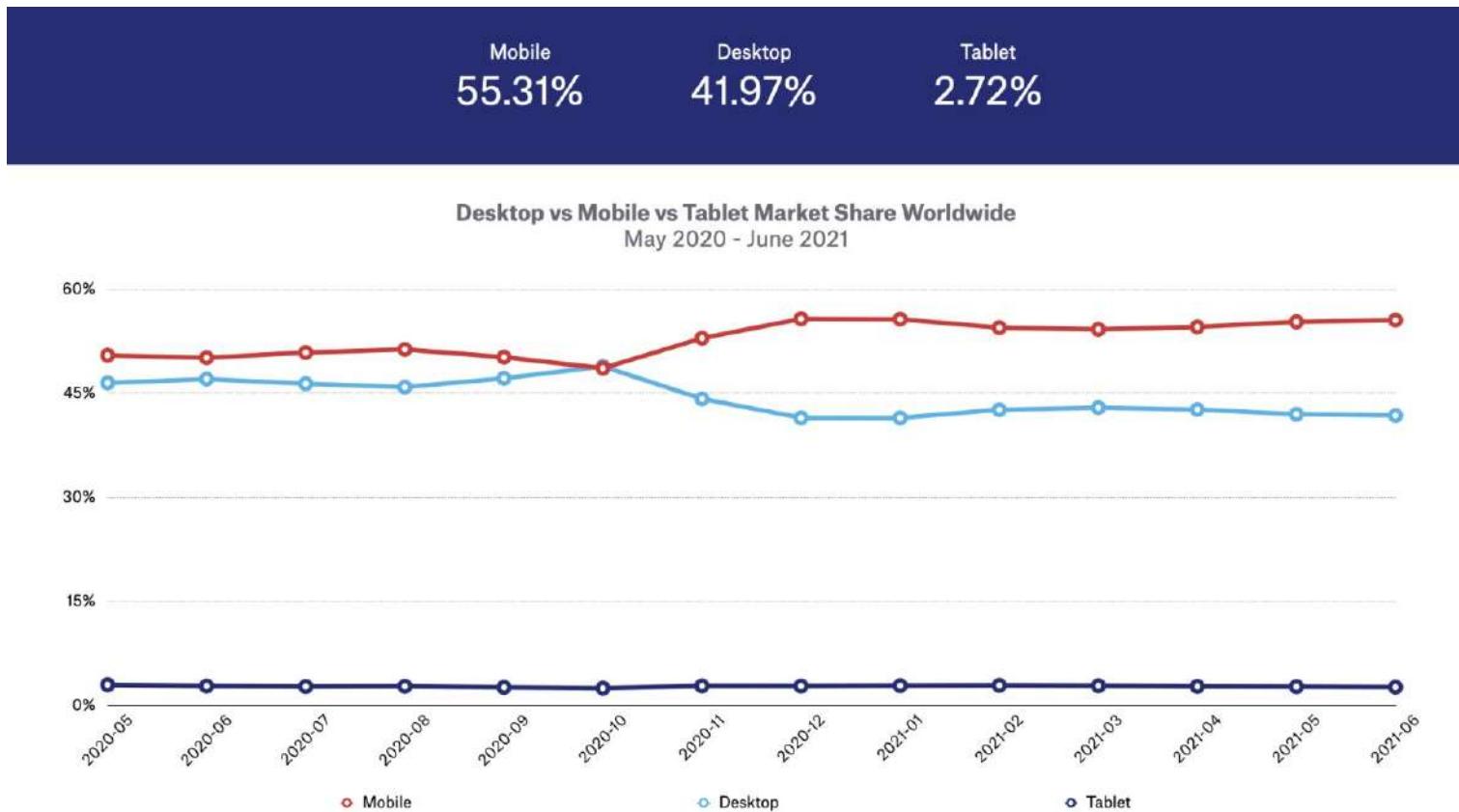
One of the most common ways to collect zip codes from customers is by asking for them at point of sale (POS).

Advertisers could then match the zip codes in store with the location data in the online ad campaign reports. Similarly with the use of zip codes for offline and online attribution, this approach is not very accurate and is best used as an addition to other attribution methods.

The Multi-Device Consumer Journey And The Technological Challenges It Presents

In the early days of online advertising, the online customer journey was undertaken on one device — predominantly desktops / laptops.

Consumers nowadays use a range of Internet-enabled devices for everything from discovering new products on social media on their laptops, to searching for flights via Google on tablets, to reading emails on smartphones.



The chart illustrates global device usage between mobile devices (e.g. smartphones), desktops and laptops, and tablets.

Source: statcounter GlobalStats

This new generation of multi-device users has given rise to the cross-device customer journey. Combine that with online and offline ads and activity and it's not hard to see why attribution is such an elusive feat for advertisers.

Attribution tools, analytics platforms, and data platforms like DMPs and CDPs can help advertisers attribute impressions and clicks to conversions across different channels and devices.

However, the growing number of privacy changes in web browsers and mobile devices mean that collecting attribution data is becoming a lot harder.

As we've seen in this chapter, attribution is an important component of improving the effectiveness of ad campaigns. But there are areas of the online advertising industry that significantly and negatively impact the performance and cost of online advertising campaigns, with **ad fraud** and **viewability** being 2 classic examples.

13. Ad Fraud and Viewability



Although the advancement of technology and growth of digital advertising has helped publishers increase revenue and allowed advertisers to reach more of their audience, it has also given rise to some very costly problems for all companies involved in digital advertising.

Two such problems are ad fraud and issues around ad viewability.

Ad Fraud

Ad fraud in digital advertising is a multi-billion dollar problem. There are many types of ad fraud, but they all work by misrepresenting advertising metrics, such as impressions, clicks, and conversions for monetary gain.

The Cost of Ad Fraud

Numerous studies show that ad fraud costs the digital advertising industry between US \$26 billion and US \$42 billion a year. To put that into perspective, global digital ad spend in 2019 was estimated to be [US \\$333.25 billion](#).

Below are some figures from recent studies into the cost of ad fraud.

\$26 billion: CHEQ, an ad fraud solution, found that ad fraud could cost the online advertising industry US \$26 billion in 2020.

\$42 billion to \$100 billion: Juniper networks estimates that ad fraud cost advertisers US \$42 billion in 2019, with this number rising to US \$100 billion by 2023.

10% to 30%: The World Federation of Advertisers estimates that 10% to 30% of advertising is not seen by consumers because of ad fraud and problems with ad viewability.

Determining the true cost and scale of ad fraud is difficult because:

1. It can be very hard to detect fraudulent activity due to the sophistication of the ad fraud techniques.
2. The technology to protect advertisers is constantly stuck in a game of cat and mouse with fraudsters.
3. Most ad fraud goes undetected and many companies choose not to publicly disclose the fact that they've been impacted by it.

All these factors mean that the actual impact of ad fraud may be higher than what is reported.

There are a number of reasons why this figure is so huge:

1. **Fraudsters follow the money.** Ad fraud moves from one lucrative area to another. The increase in ad spend has attracted more fraudulent behavior. You'll often see an increase in ad fraud in emerging areas of digital advertising, such as mobile in-app and OTT/CTV (more on this below).
2. **Digital advertising is less regulated than the financial industries,** meaning it's easier for fraudsters to get away with their criminal activities.
3. **The digital advertising ecosystem is fragmented and complex,** which makes it easier for fraudsters to conceal their activity.

The Main Types of Ad Fraud

What makes online ad fraud so challenging is that there are several ways to steal money from advertisers and publishers, with new ad fraud methods being created all the time.

The most common ad fraud techniques include:

Invisible and Hidden Ads

With this ad fraud technique, ads will be invisible or hidden on websites, but an impression will still be recorded.

There are a few ways fraudsters can carry out this technique:

- Display an ad in a 1×1 pixel iframe.
- Display ads outside of the viewport area.
- Display (multiple) re-sized ads.
- Display several ads in an iframe loaded to a single ad slot so that out of all the ads loaded, only one will actually be visible to the user. This is also known as ad stacking.

This technique is not the same as non-viewable impressions (see below) whereby ads are displayed on a website and recorded but aren't seen by a user because they're at the bottom of the page where the user doesn't scroll to.

Domain Spoofing

Domain spoofing involves a fraudulent website disguising itself as a genuine and often premium website. Some fraudulent AdTech platforms can also carry out domain spoofing.

Brands pay high CPMs to display their ads on premium websites or websites where their target audience is, so by disguising itself as one of these websites, fraudsters can take the ad revenue that should have gone to the real website.

Ad Injection

Also known as hijacked ads, this type of ad fraud injects ads into unsuspecting websites, usually via malicious browser plugins or mobile apps.

Ad injection can be done in a few ways:

- Compromising the user's computer to change the DNS resolver — e.g. by resolving the ad.doubleclick.com domain to the IP of the server controlled by the attacker and therefore serving different ads.
- Compromising the publisher's website or the user's computer to change the HTML content on the fly — e.g. changing ad tags placed by the publisher to tags controlled by the attacker.
- Compromising the user's proxy server or router (or the ISP's router) to spoof the DNS server or change the HTML content of the site on the fly.

Click Injection

Click injection, also known as hijacked clicks, is a similar technique to ad injection, but instead of injecting ads into a web page, fraudsters will inject clicks. The way fraudsters make money is by receiving money for the click and also the conversion.

So instead of the commission for a conversion going to a genuine publisher or mobile app, it would go to the fraudster as their fake click would be recorded as the last touch before the conversion.

Cookie Stuffing

The cookie-stuffing technique is used to steal money from CPA or affiliate marketing campaigns.

Because cookies are often used to attribute conversions, fraudsters will stuff a user's browser with cookies they've either created themselves or have stolen from other publishers. This allows them to receive commissions from affiliate networks when a user completes a conversion on a publisher's websites (e.g. purchases a product).

How Ad Fraud Is Carried Out

The above types of ad fraud can be carried out in many ways:

Bot traffic: Non-human traffic generated by botnets, which consist of compromised computers, cloud servers, and proxy servers. This type of traffic is often referred to as sophisticated invalid traffic (SIVT).

Click farms and device farms: A collection of devices (laptops and mobile phones) used to generate fraudulent impressions, clicks, and conversions (e.g. app installs). These farms are sometimes operated by humans or via programs installed on the devices.

Methbot and 3ve

Although there are many botnets and types of malware, the most costly botnets ever discovered are Methbot and 3ve.

These botnets were elaborate and sophisticated operations that stole an estimated US \$36 million from advertisers between 2014 and 2018.

Ad fraud is rarely investigated by law enforcement, but in November 2018 the [US Department of Justice \(DoJ\) issued a release](#) saying it has indicted 8 people over the Methbot and 3ve schemes.

The investigation is the largest criminal investigation into ad fraud that has ever taken place and involved the FBI, the US Department of Homeland Security, and private companies including Google and White Ops.

Ad Fraud in Emerging Areas of Digital Advertising

Although ad fraud began in the display advertising world, it has moved into other emerging areas of digital advertising such as mobile in-app and OTT/CTV.

Mobile In-App Ad Fraud

Many of the ad fraud techniques used in web browsers are also found in mobile in-app environments. But there are a few that are specific to mobile in-app.

App or SDK spoofing: Similar to domain spoofing, this technique tricks advertisers into thinking that their ad will appear in a premium app, when it will actually appear in a fraudulent app.

Ad stacking: Ads are placed on top of one another so the app earns more ad revenue, but only one ad is displayed to the user.

Click injection: Just like click injection in web browsers, fraudsters collect ad revenue and affiliate commissions for clicks they didn't generate themselves.

Hidden ads: Fraudsters run ads in the background of apps, giving off the impression that they are being displayed to users when they aren't.

Malware: Malicious apps that carry out one or more of the above techniques to generate fraudulent ad revenue.

OTT & CTV

The over-the-top (OTT) and connected TV (CTV) industries are ripe for ad fraud; they are emerging and growing areas of digital advertising with higher CPMs than other channels, there's no direct connection between buyers and sellers, there's a lack of transparency, and brands are pouring more money into them.

Pixalate, an ad fraud intelligence and marketing compliance company, recently uncovered two ad fraud schemes in the OTT/CTV environment. Pixalate has named these schemes [DiCaprio](#) and [Monarch](#).

The DiCaprio ad fraud scheme used similar techniques found in web browsers and mobile apps to fool advertisers into thinking that they were bidding on inventory on Roku devices.

It seems that fraudsters compromised the security of the popular social networking app Grindr to send out ad requests via a script, which contained the name DiCaprio.

The ad requests appeared to come from Roku apps on Roku devices. Advertisers would bid on these ad requests believing their ads would be shown to Roku users, when in fact they would run in the background inside the Grindr app.

The Monarch scheme used a spoofing technique to make it appear that ads would be displayed on premium Roku apps, when actually they would end up on non-premium apps like screensavers. Unlike the DiCaprio scheme that involved mobile devices, the Monarch scheme was contained to Roku apps and devices.

In another ad-fraud scheme, known as [Icebucket](#), detected by bot-mitigation company White Ops, fraudsters impersonated more than 2 million people and generated 1.9 billion ad requests on OTT/CTV and mobile devices.

The scheme used a botnet to produce artificial viewing activity on edge devices (mainly mobile and CTV devices).

How Advertisers And Publishers Can Defend Against Ad Fraud

Combating ad fraud is an ongoing battle, but there are a couple of things publishers, brands, agencies, and AdTech companies can do to reduce ad fraud.

1. Use Ad Fraud Detection Software

There are several software companies that detect and prevent many of the ad fraud techniques listed above for different advertising channels. Many AdTech companies also provide ad-fraud detection features as part of their offering.

Below are some of the main cybersecurity and ad-fraud detection companies:



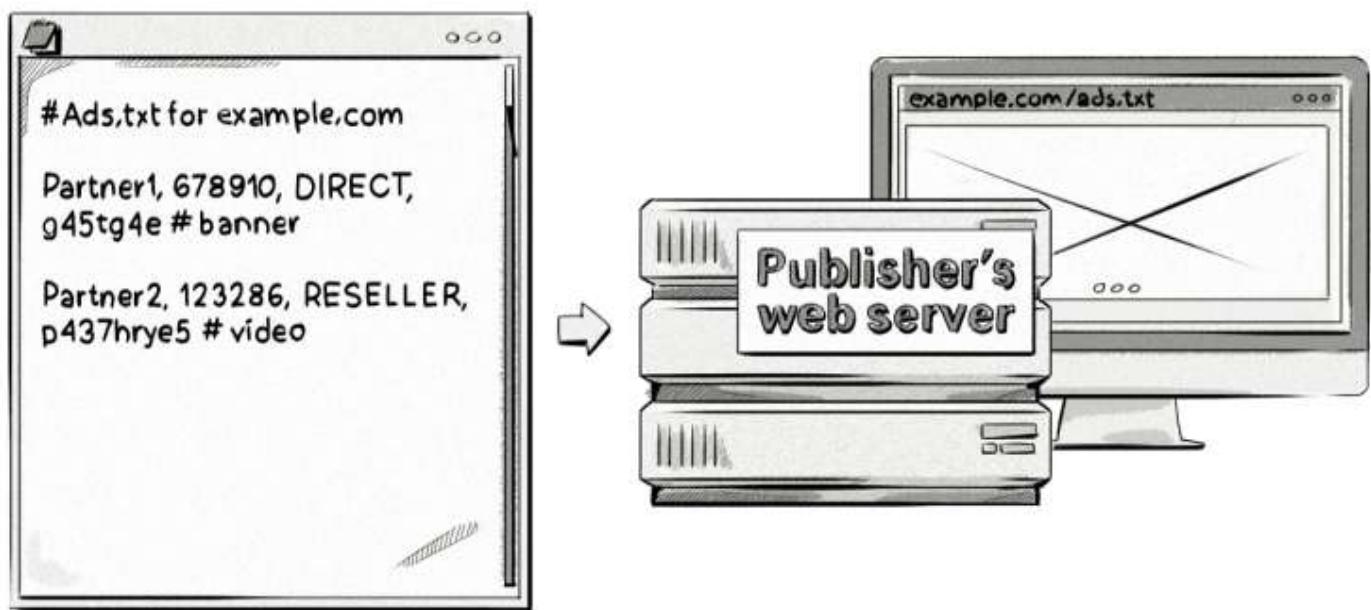
2. Adopt IAB standards

Over the past few years, the IAB have produced a number of standards to help reduce ad fraud in web browsers and mobile apps. These include **ads.txt**, **app-ads.txt**, and **sellers.json**.

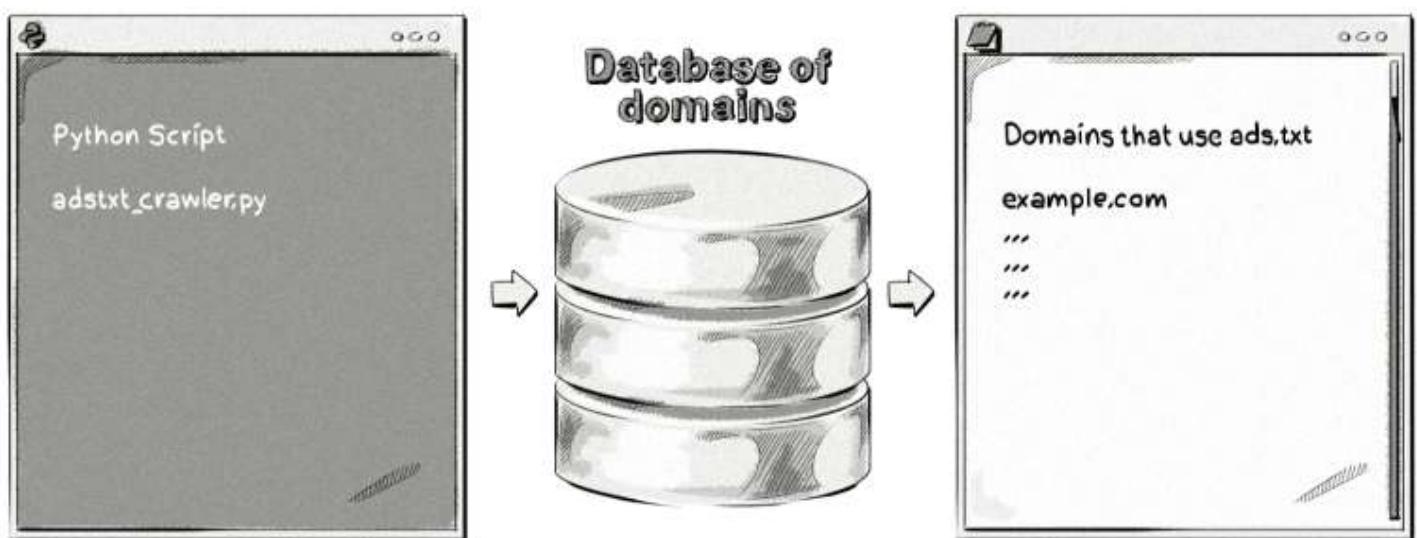
Authorized digital sellers (ads.txt)

Ads.txt aims to tackle domain spoofing (a type of ad fraud) and arbitrage, which is a process where impressions are bought and then repackaged and resold at a higher price by a third party. Ads.txt helps to solve this problem by indicating who the authorized sellers and resellers of a publisher's inventory are.

To adopt the standard, a publisher adds an ads.txt file containing information about all the programmatic partners (supply-side platforms, ad exchanges, ad networks, etc.) they work with to their web server and host it under their root domain.



Advertisers or AdTech companies can then use a script to crawl the web (or a database of domains) to collect the ads.txt files from publishers.



Advertisers can then reference a publisher's ads.txt file against IDs in OpenRTB bid requests. If there's a match, then advertisers can be assured that they are buying inventory from genuine publishers.

You can see whether a publisher has an ads.txt file and view the contents of it by adding /ads.txt to the end of a root domain, e.g. businessinsider.com/ads.txt and cnn.com/ads.txt.

The breakdown of an ads.txt entry

AdTech partner	Seller Account ID	Direct or reseller	Certification Authority ID (optional)	Inventory type (optional)
google.com, pub-5425784415875548	DIRECT	f08c472356fc5c8fc	#banner	

Here's a breakdown of the information in the above ads.txt entry:

AdTech partner – The AdTech platform, typically supply-side platforms and ad exchanges, the publisher uses to sell their inventory. Examples include [google.com](#) [appnexus.com](#), [bidfluence.com](#), [rubiconproject.com](#) and [pubmatic.com](#).

Seller Account ID – This represents the publisher's account ID for the respective AdTech vendors and is used to verify the authenticity of the inventory during RTB auctions.

Direct or reseller – Direct means that the publisher works directly with the AdTech vendor to sell its inventory. Reseller means that the publisher has authorized another company to sell its inventory on its behalf. For example, SSP2 (reseller) could sell the publisher's inventory via SSP1 (direct).

Certification Authority ID – This optional field represents the advertising system within a certification authority, for example, the Trustworthy Accountability Group (TAG).

Inventory type – Some publishers include this optional field so they know which type of inventory the AdTech vendor sells (view [cnn.com/ads.txt](#) to see examples). As this hashtag represents a comment, it won't be picked up by the crawling script unless certain configurations are made to it, but as this is purely for the publisher's benefit, there's no real need for buyers to have this information.

Authorized digital sellers for apps (app-ads.txt)

App-ads.txt is the mobile app version of ads.txt, but with a few differences in the setup.

To adopt app-ads.txt, app developers need to provide a developer website URL in app store listings and publish an app-ads.txt file. App stores are also encouraged to publish three HTML <meta> tags with the store listing page for each individual app to allow advertisers and AdTech companies to match the bundle_id and/or store_id in bid requests.

Here's an example of the three HTML meta tags provided by the IAB:

```
<meta name="appstore:developer_url" content="https://www.path.to/page" />
<meta name="appstore:bundle_id" content="com.example.myapp" />
<meta name="appstore:store_id" content="SKU12345" />
```

Advertisers and AdTech companies then need to crawl app listing pages in app stores to retrieve these three HTML meta tags, translate the developer URL to an app-ads.txt path, and then crawl the web for the app-ads.txt file and interpret them.

Ads.cert

Ads.cert is considered a more secure version of ads.txt and aims to increase transparency into programmatic ad buying by providing cryptographically signed bid requests. By doing so, media buyers can be sure that the information being sent in the bid request (e.g. the publisher's URL, user's location, user's IP, and user's device) is factual.



Here's how the process works, step by step (steps based on the [IAB Tech Lab's documentation](#)):

1. OpenSSL's security software is used by the publisher to generate a pair of [ECDSA](#) keys based on the bid request:
 - Public (secured, yet accessible, to be read by systems which validate the bid request against the signatures). The Public Key file must be shared via HTTP and/or HTTPS from the

- publisher's website under a relative path on the server: /ads.cert. Although ads.cert is referred to as a file, the resource does not need to come from a file system.
- Private (secret, secure, and inaccessible to outside systems, yet accessible to the systems that generate and sign bid requests, e.g. SSP). Private keys are in a standard format known to compatible security packages.
2. An encrypted signature based on the bid request is generated with a private key and attached to the bid request and sent out on behalf of the publisher by an SSP, with [details](#) about the impression available, publisher's website or app, industry, language, etc.
 3. The recipient of the request will then use the public key to generate another signature for that same bid request.
 4. The signatures generated by the publisher and by the recipient are compared to check if they were generated based on the same bid request (created using a matching pair of keys). If yes, then the bid request is considered legit. Any alterations of the signed elements can be detected by the recipient or other servers in the chain.

The main drawback of ads.cert is that it's only available with OpenRTB 3.0, which is not currently supported by a majority of AdTech platforms.

Sellers.json and the OpenRTB Supply Chain Object

Sellers.json allows media buyers to see all the sellers and resellers involved in a bid request. In many ways, sellers.json is an extension to ads.txt. So instead of just seeing a list of authorized sellers and resellers in an ads.txt file, sellers.json lists the final seller of a bid request.

The OpenRTB Supply Chain Object is part of sellers.json and provides a record of all the sellers (direct) and resellers that have been involved in bid requests.

By viewing all of the entities (referred to as nodes) involved in bid requests, media buyers can get more transparency into the supply chain, identify whether the entities are partners they want to work with, and see how many entities the bid passed through before it was delivered to publishers.

Ad Viewability

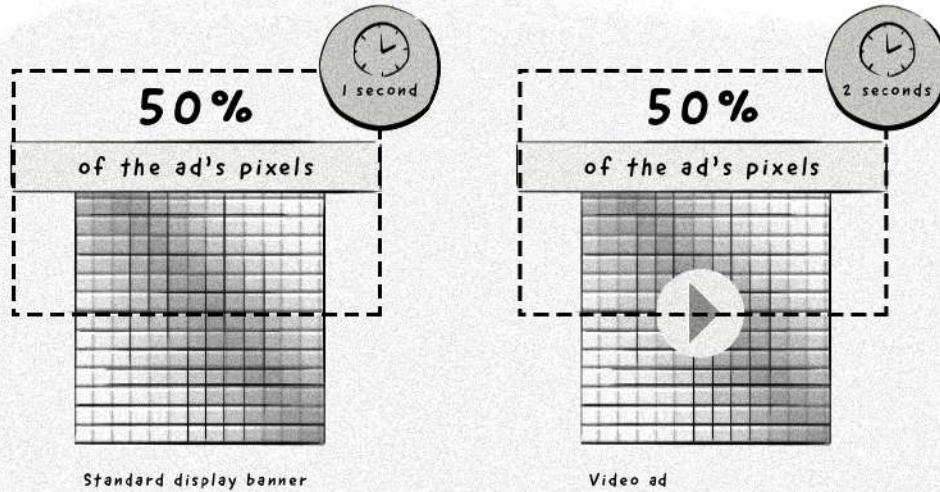
Ad viewability refers to whether an ad was seen by a human or not.

Although non-viewable ads can be a result of ad fraud, such as if a publisher uses bots to generate impressions, in most cases the reason is not sinister, for example if an ad is located at the bottom of a page where a user doesn't scroll to.

Ad viewability is one of the biggest issues in today's online advertising world with some sources stating that [over half of all ads served](#) are not actually viewed by an online user.

A large majority of AdTech platforms do a pretty good job of determining whether an ad has been served and whether an ad has been clicked on, but determining whether an ad was actually viewed by a user can be hard to measure.

The current industry standard provided by IAB and the Media Rating Council (MRC) states that for an ad to be registered as viewed, it needs to have met these two criteria:



Source: MRC Viewable Ad Impression Measurement Guidelines, Version 1.0 (Final) – June 30, 2014
<https://www.iab.com/guidelines/iab-measurement-guidelines/#mrcviewable>

For display ads: 50% of the ad's pixel needs to be in the web browser's viewport for a minimum of 1 second.

For video ads: 50% of the ad's pixel needs to be in the web browser's viewport for a minimum of 2 seconds.

Viewable Impressions

As we saw in the ad server chapter, impression trackers are used by both advertisers and publishers to track the number of impressions an ad receives.

However, this only tracks impressions that are served; it doesn't tell us if the ad was actually viewed by a user. So not only do you need to track the number of impressions served, you also need to determine if the impression was actually seen by a real user.

Ads may be served but not viewed because of one or more of the following reasons:

- The ad may have taken too long to load, leaving a blank space where the ad should have been.
- The user could have scrolled down or switched tabs or windows before an ad could be displayed to them.
- The user could be using an ad-blocking plugin like AdBlockPlus, uBlock, or Ghostery.
- There might have been some technical issues with the webpage or web browser.

Also, there are a number of fraudulent long-tail sites that perform all kinds of tricks to record an ad impression, when in fact, the ads could never be seen on the page at all.

What is a long-tail website?

A long-tail website refers to a small publisher or individual blogger.

Typically, these sites will monetize their site with Google AdSense and the inventory on these sites is known as long-tail inventory.

A lot of hope is placed in the so-called **viewable impression**.

The idea behind viewable impression is pretty straightforward:

An advertiser pays only for ad impressions that were actually seen by a user.

Sounds simple, but the problem is much more complex when analysed from the technical perspective.

Luckily, companies like Google, DoubleVerify, IAS, and Moat offer ad viewability measurement software to help advertisers determine how many of their ads were actually viewed by users.

Chapter Summary

- Ad fraud costs the digital advertising industry between [US \\$26 billion](#) and [US \\$42 billion](#) a year.
- The most common types of ad fraud in web browsers are:
 - Invisible and hidden ads.
 - Domain spoofing.
 - Ad injection.
 - Click injection.
 - Cookie stuffing.
- Ad fraud is also a problem with mobile in-app advertising and is emerging in growing areas of digital advertising like OTT/CTV.
- Companies can detect and reduce ad fraud by using ad fraud detection software and adopting IAB standards like ads.txt, app-ads.txt, ads.cert, and sellers.json.
- Ad viewability refers to whether an ad was seen by a human or not.
- Ad viewability is one of the biggest issues in today's online advertising world with some sources stating that [over half of all ads served](#) are not actually viewed by an online user.
- IAB and the Media Rating Council (MRC) states that for an ad to be registered as viewed, it needs to have met these two criteria:
 - Display ads: 50% of the ad's pixel needs to be in the browser's viewport and seen for a minimum of 1 second.
 - Video ads: 50% of the video needs to be visible and seen for a minimum of 2 seconds.
- Viewable impressions refers to ad impressions that meet the criteria above and are actually seen by a user.

14. User Privacy in Digital Advertising



Throughout history, advertising has followed the consumer through the invention and rise of new mediums, from the print world to the online world.

But the world of online advertising has brought with it a number of issues that have caused companies, governments, and consumers to take a proactive approach to limiting the amount of user data that can be collected.

In this chapter, we'll look at one of the biggest topics in programmatic advertising; **user privacy**.

The Rise of Consumer Data Collection and Privacy Concerns

In the early days of online advertising, ad targeting was limited to the context of the page and information passed to ad servers and ad networks in the user agent string (passed in a HTTP header) by web browsers, such as:

- The language set on the user's computer.
- The URL of the page where the ad will be displayed.
- The browser type and version.

- The user's operating system.

When RTB emerged in the late 2000's, AdTech companies started ramping up the use of third-party cookies to identify users across different websites and display ads to them based on their interests and behavior.

Nowadays, user data can be collected in several ways and combined with data collected from different sources to improve ad targeting, measurement, attribution and conduct frequency capping.

The amount of user data collected by AdTech and data companies has increased significantly over the years, which has given rise to concerns about how companies are collecting this data and what they are doing with it.

*To learn about how users are identified, the types of data that AdTech companies collect, and how data is collected, read chapters **10. User Identification** and **11. Data Management Platforms (DMPs) and Data Usage**.*

The user privacy topic in AdTech is made up of privacy laws (e.g. the GDPR and CCPA) and privacy settings and technical limitations (e.g. ad blockers and web browser settings).

Privacy and Data Protection Laws Around The World

More and more users are becoming concerned about the collection, use, and distribution of their online data. Many are also worried that their privacy is being invaded and exploited by online advertising companies.

In this section, we'll look at the various privacy and data laws in the US and Europe.

The European Union's General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), or Regulation (EU) 2016/679 as it's known in official contexts, is a regulation spearheaded by the three legislative European Union institutions: the European Parliament, European Commission, and Council of the European Union.

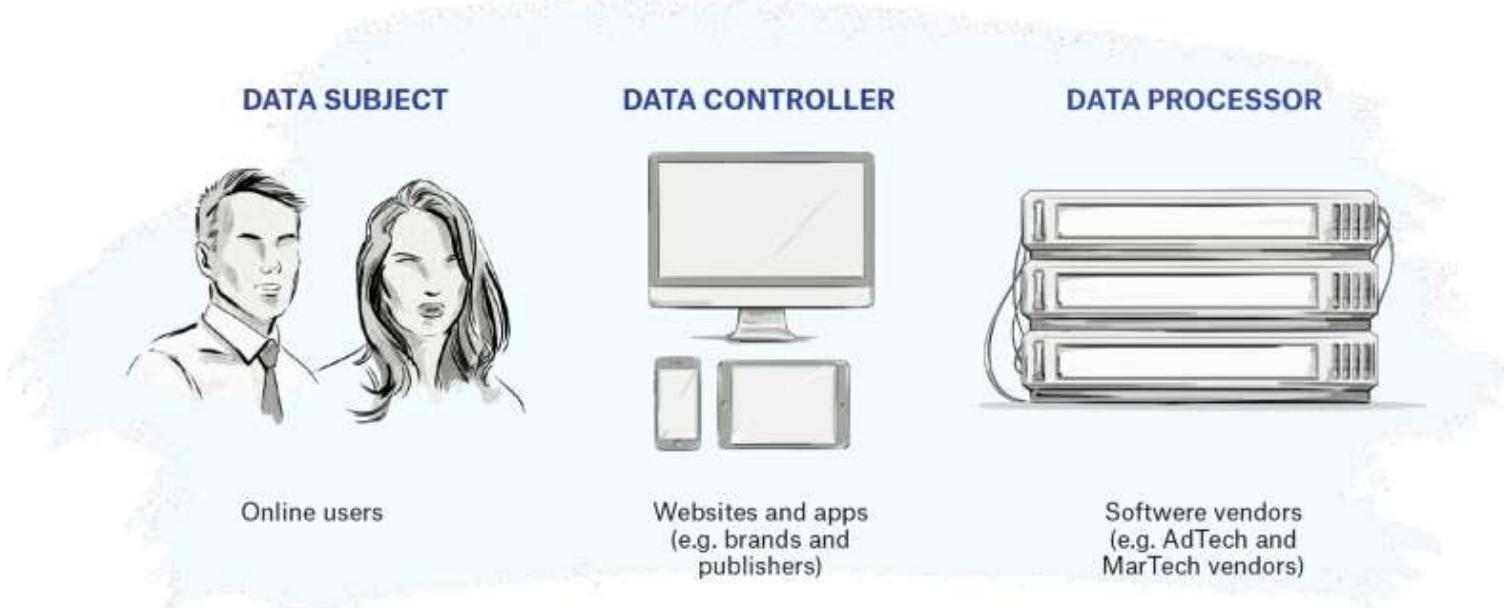
It replaced the Data Protection Directive (Directive 95/46/EC) when it came into force on May 25, 2018.

The GDPR aims to protect the data and privacy of citizens and residents of the European Union member states (highlighted in light blue). Even though Norway, Iceland, and Liechtenstein (highlighted in dark blue) are not EU member states, they are European Economic Area (EEA) members and are also included in the GDPR.



Key Terms of the GDPR

Below are three key terms that relate to online advertising and marketing: **data subject**, **data controller**, and **data processor**.



Data Subject

The GDPR defines a data subject as a *natural person whose personal data is processed by a controller or processor*.

In the context of digital advertising, a data subject is an EU or EEA citizen or resident whose data can be collected by AdTech companies.

Data Controller

A data controller is any person or company that collects data about EU citizens and residents.

Examples include publishers, ecommerce stores, individual bloggers, brands, and companies that collect data about users either directly or indirectly via another company.

Data Processor

A data processor is any person or company that provides services or technology and collects data on behalf of data controllers.

Examples include AdTech and MarTech vendors.

Personal, Pseudonymous, and Anonymous Data

Another key term in the GDPR is **personal data**.

In simple terms, if a piece of information, either separately or combined with other pieces of data, can be used to identify a person, then it's classed as personal data.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Article 4 (1)

GDPR

Identity in this sense doesn't just refer to knowing a person's name, it also refers to identification.

This means if a user visits your website or sees one of your ads, they are considered identifiable if you can later recognize them, e.g. by identifying and recognizing them via their cookie ID or other identifier, if they return to your website or see another one of your ads.

The same principle applies to singling out an individual based on several data points, such as their postal code, gender, and age. In this case, even though you don't know the person's name or have an identifier, e.g. a user ID in a cookie saved in their browser, you could still potentially identify them.

In the past, AdTech vendors and most MarTech vendors have based their privacy policies on the fact that they are not collecting or dealing with personal data because online identifiers, such as cookie IDs, IP addresses, device advertising IDs, and device fingerprints were not considered examples of personal data.

However, under the GDPR, any piece of data or information that can in some way identify a person is classed as personal data.

Apart from personal data, the GDPR also refers to two other types of data: **pseudonymous** and **anonymous**.

Pseudonymous data refers to data that's been changed into a non-identifiable format, rendering it unable to identify a person without the use of additional data, such as the hashing function or encryption keys.

'Pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Article 4 (5)

GDPR

Anonymous data means that it can't be used to identify a person, which, for this reason, offers little value to online advertising and marketing companies as they are in the business of identifying people and targeting them with ads and marketing messages.

Due to its inability to identify a person, anonymous data is not subject to the rules of the GDPR, meaning if a company collects anonymous data, they don't have to obtain user consent.

...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.

Recital 26

GDPR

A Comparison of the Three Types of Data

Below is a comparison table that provides examples of personal, anonymous, and pseudonymous data.

Type of Information Collected	Personal Data	Pseudonymous Data	Anonymous Data
Device information	AEBE52E7-03EE-455A-B3C4-E57283966239 Device advertising identifier (e.g. Apple's IDFA - Identifier for Advertising)	e69a1078552e13f2734c22322708bd95 Device advertising identifier Using a one-way hash function to convert the data into a non-identifiable format. The device can be re-identified by applying the same hash function to the original value and comparing it to the pseudonymous hash.	Apple iPhone 7 <i>Device brand and model</i>
Email address	john.smith@company.com Email address	1bc5edb4799fd8eec67c66122f47eb73 Email address Similar to the advertising one-way hash function.	company.com <i>Domain of the email address</i>
Web activity	213.86.17.58	8d61a1f53fdc1b74.1495187	500+ pageviews

(e.g. pageviews)	<p>https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/</p> <p style="text-align: center;">/</p> <p>(URLs visited)</p> <p>A list of page URLs visited on a website along with an IP address of the visitor.</p>	<p>199.51.1505818713.150581</p> <p>7299.</p> <p>https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/</p> <p>(URLs visited)</p> <p>A list of page URLs visited on a website along with a randomly generated unique identifier that has been set in the visitor's browser cookie.</p>	<p>http://clearcode.cc/about/</p> <p>An aggregated number of times a given page was viewed</p> <p>https://clearcode.cc/ https://clearcode.cc/about/ https://clearcode.cc/contact/</p> <p>(URLs visited)</p> <p>A list of the page URLs visited on a website without containing cookie IDs, IP addresses, or any other personally identifiable information.</p>
Address and DOB	<p>742 Evergreen Terrace Henderson, NV 8901 USA</p> <p>Address</p> <p>November 24, 1971</p> <p>Date of birth</p>	<p>1971 NV 8901</p> <p>The year of birth and a postal code.</p> <p>By using an external database, a data subject can be re-identified, hence the data cannot be considered anonymous.</p>	<p>89**</p> <p>Suppressing certain parts of the data, e.g. removing the last two digits of a postcode.</p> <p>45-54</p> <p>Age range instead of the exact age.</p>

The column on the left contains different types of user information, then shows how the data would look under the different categories of data: personal data, anonymous data, and pseudonymous data.

From the table above, it appears that anonymous data is the least likely to expose the identity of a data subject.

While that is true in most cases, it's important to keep in mind that the anonymized data could still be linked to an individual if enough pieces of data are combined together.

For example, having a single data point, like an age range of 40–50, out of a sample size of 1,000 couldn't be linked to an individual, but when you add in other anonymized data sets (e.g. postcodes and the year of birth) and combine with other sets of data (e.g. public records or data), it can easily become personal data and could be used to identify an individual.

Did you know?

There have been a number of situations of anonymized data becoming re-identifiable, with one example being [Netflix's 2006 contest](#) in which the company put up a \$1 million prize for the person or team who could significantly improve their recommendation algorithm. As part of the content, Netflix released 10 million movie rankings by 500,000 customers, which included the following information:

- A unique subscriber ID
- Movie title
- Year of release
- The date on which the subscriber rated the movie

Even though personally identifiable information, such as customer name, was replaced with a unique ID, two researchers at the University of Texas at Austin, Arvind Narayanan and Vitaly Shmatikov, were able to de-anonymize some of the data and identify certain users by comparing user ratings and the date on which they rated the movies with information from the site Internet Movie Database (IMDB).

A Side Note About Sensitive Data

The GDPR also includes another type of data class: **sensitive data**.

Examples of sensitive data include religious or philosophical beliefs, racial or ethnic origin, political opinions, trade-union membership, and data concerning health, sex life, and sexual orientation.

Sensitive data is typically not collected by advertisers or marketers as it requires stronger grounds for processing and is subject to additional protections, meaning the payoff just isn't viable.

Advertisers and marketers wishing to collect, store, and use sensitive data should be aware that they will need to obtain explicit consent from the data subject.

What Does This Mean for AdTech From a Technical Perspective?

The definition of personal data is somewhat unchanged from the definition given in the Directive; however, it broadened the scope of the data-protection law.

One example of the change in scope is that the GDPR now considers online identifiers and location data as personal data.

As most online advertisers, marketers, and publishers collect and use online identifiers, such as those mentioned above, as well as location data, they will now have to take additional steps to ensure they are compliant with the GDPR's rules regarding the collection, storage, and usage of personal data.

Examples of personal data include:

- Names
- Email, home, and work addresses

- Phone numbers
- Cookie IDs (visitor identifiers stored in cookies)
- IP addresses
- Device IDs
- Device fingerprints

The GDPR states that companies collecting personal data should implement measures to ensure the data is protected at all times, for instance, via encryption and pseudonymization.

Although most companies already do this with obvious examples of personal data, such as emails, phone numbers, and IP addresses, they now have to apply this to all types of data they collect.

While these measures will help online advertising and marketing companies mitigate risks associated with data security, encrypted and pseudonymized data are still classed as personal data, meaning companies still have to obtain user consent and carry out various data-protection measures if they wish to collect and use the information.

The main challenges advertising and marketing companies face with personal data are collecting it in the first place (i.e. obtaining consent), ensuring its security, and creating a chain of responsibility with their partners when they exchange data with them.

The European Union's ePrivacy Directive

The ePrivacy directive is a piece of EU legislation that also aims to protect the data and privacy of EU and EEA citizens and residents, but with a focus on respecting their private lives when using electronic communications.

Within the online advertising and marketing industries, the current ePrivacy directive is often conversationally referred to as the **cookie law** because it regulates the usage of cookies, among other identifiers.

However, it relates to the protection of privacy in the electronic-communications sector as a whole, not just the usage of cookies for online advertising and marketing.

One of the most prominent consequences of the ePrivacy directive (officially known as the Privacy and Electronic Communications Directive, 2002/58/EC) is the cookie-consent notices — also known as **cookie bars** — like the one below from bbc.co.uk:

Cookies on the BBC website

The BBC has updated its cookie policy. We use cookies to ensure that we give you the best experience on our website. This includes cookies from third party social media websites if you visit a page which contains embedded content from social media. Such third party cookies may track your use of the BBC website. We and our partners also use cookies to ensure we show you advertising that is relevant to you. If you continue without changing your settings, we'll assume that you are happy to receive all cookies on the BBC website. However, you can change your cookie settings at any time.

✓ Continue ⚙ Change settings ⓘ Find out more

A common identifier of the current EU ePrivacy directive is the cookie-information banners displayed to EU citizens, which will likely be superseded by a new user-consent form under the GDPR and ePrivacy regulations.

Currently, ePrivacy is a directive, but is in the process of being transformed into a regulation, which will also repeal the current directive.

Once adopted, ePrivacy will regulate the processes of placing, accessing, and using identification technologies on users' devices based on the broadened definition of personal data as recognized by the GDPR (e.g. cookies, device advertising IDs, and IP addresses).

It is not known when the ePrivacy regulation will come into force as the proposal is set to be negotiated between the three EU legislative institutions (see below).

Given that it is still in progress, the final version of the ePrivacy regulation may still affect how AdTech platforms interact with online identifiers based on the GDPR itself and the current state of ePrivacy.

What's the difference between GDPR and ePrivacy?

Both the GDPR and ePrivacy are based on Articles of the EU Charter of Fundamental Rights, a document containing the rights and freedoms protected in the EU.

The GDPR is based on Article 8 and relates to the protection of personal data, whereas ePrivacy is based on Article 7 and relates to respect for private life.

In simple terms, the GDPR is focused on data protection, and ePrivacy is focused on the right to respect a data subject's private and family life, home, and communications.

Also, ePrivacy is *lex specialis* of the GDPR, meaning that when the two regulations cover the same situation, ePrivacy will override the GDPR.

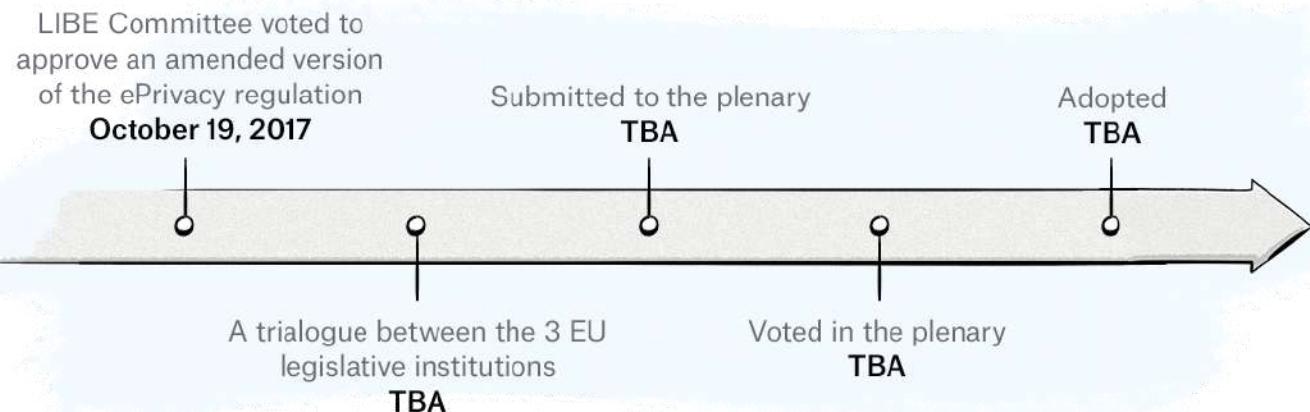
The Current State of ePrivacy

In December 2016, a draft of the proposed ePrivacy regulation was leaked, with the first official draft formally released by the European Commission in January 2017.

On October 19, 2017, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (aka LIBE Committee) voted to approve an amended version of the ePrivacy regulation. This amended version was then approved by members of the European Parliament during a plenary session (a meeting of the whole Parliament).

Another draft was released in March 2019, with subsequent proposals released in [March 2019](#) and [November 2019](#).

The drafts have been met with some strong opposition from various advertising and marketing organizations, including the [Interactive Advertising Bureau Europe \(IAB Europe\)](#) and [Digital Europe](#) — whose members include Google, Apple, Microsoft, and IBM — with their main concerns centered around the lawfulness of data processing based on the notion of legitimate interest.



Once the draft has been finalized, the next stage involves trilogue negotiations between representatives of the European Parliament, the Council of the European Union, and the European Commission. Once the proposal is finalized and approved by way of voting, it will be adopted and enforced.

California Consumer Privacy Act of 2018

The California Consumer Privacy Act (CCPA) is a law passed by the California State Legislature on June 28, 2018 and came into effect on January 1, 2020. Enforcement of the act began on July 1, 2020.

The goal of the CCPA is to make it easier for Californian citizens and residents to know the types of personal information businesses collect about them, and give them the right not to agree to the sale of their personal data to other parties

The CCPA provides Californian citizens and residents with the following rights:

- Right to know all the data a business collects about them.
- Right to say NO to the sale of their information.
- Right to DELETE their data.
- Right to be informed of what categories of data will be collected about them prior to its collection, and to be informed of any changes to this collection.
- Mandated opt-in before sale of children's information (under the age of 16).
- Right to know the categories of third parties with whom their data is shared.
- Right to know the categories of sources of information from whom their data was acquired.
- Right to know the business or commercial purpose of collecting their information.
- Enforcement by the Attorney General of the State of California.
- Private right of action when companies breach their data.

What are the Non-Compliance Fines?

Under the CCPA, fines are enforced by the California Attorney General and can reach up to \$7,500 per every violation (in the case of intentional violations). Non-intentional violations remain subject to the \$2,500 maximum fine.

Also, the CCPA allows affected consumers to take individual or class-action lawsuits against offending businesses, which should be a more serious financial concern for potential violators. Damages range between \$100 and \$750 – or more, if actual damages are proven.

The Definition of Personally Identifiable Information (PII) and Personal Data

Personally Identifiable Information (PII) is a term regularly used in AdTech, but it extends well past this industry.

In fact, PII is often referenced by US government agencies, such as the [National Institute of Standards and Technology \(NIST\)](#).

NIST provides the following definition of PII:

PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

A very similar definition is provided by [US Government's Office of Management and Budget](#):

The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

What Pieces of Information are Considered PII?

PII can be divided into two categories: **linked information** and **linkable information**.

Linked information is any piece of personal information that can be used to identify an individual and includes, but is not limited to, the following:

- Full name
- Home address
- Email address
- Social security number
- Passport number
- Driver's license number
- Credit card numbers
- Date of birth
- Telephone number
- Internet protocol (IP) address

Linkable information, on the other hand, is information that on its own may not be able to identify a person, but when combined with another piece of information could identify, trace, or locate a person.

Examples of personally identifiable information (PII)



Names



john@example.com



742 Evergreen Terrace



(718) 628-8700

Postal addresses

Phone numbers

Here are some examples of linkable information:

- First or last name (if common)
- Country, state, city, postcode
- Gender
- Race
- Non-specific age (e.g. 30-40 instead of 30)
- Job position and workplace

Non-PII

There's a lot of grey area around whether identifiers like cookie IDs and device IDs are examples of PII or non-PII.

While the definition of PII doesn't include a specific reference to cookie IDs or device IDs, the [Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#) from the NIST suggests that they are classed as PII (emphasis ours):

Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.

However, many AdTech companies, advertisers, and publishers class cookie IDs and device IDs as non-PII.

The screenshot shows a browser interface with a sidebar on the left listing various cookies. A specific cookie, 'IDE', is selected, and its details are shown in a modal window. The modal has columns for Name, Value, and Domain. The Value column contains a long alphanumeric string, and the Domain column shows '.doubleclick.net'. An annotation with an arrow points from the text 'The data contained in a cookie created by Google' to the Value field.

Name	Value	Domain
IDE	AHWqTUKSbjDBusNSudXCq8TTV6WCebD6CAbA7B8SVjmMZXNxZcDr...	.doubleclick.net

A list of cookies on the page

The data contained in a cookie created by Google

One could argue that cookie IDs and device IDs can be deleted or reset and therefore aren't persistent forever, but the same could be said for other types of PII such as home addresses, email addresses, and password numbers that can change more than once during a person's life.

The Definition of Personal Data

As we mentioned above in the section about the GDPR, personal data is a term used in the European Union to define a piece of information that can be used to identify a person.

Examples of personal data include:

- Names
- Email, home, and work addresses
- Phone numbers
- Cookie IDs (visitor identifiers stored in cookies)
- IP addresses
- Device IDs
- Device fingerprints

What's the Difference Between PII and Personal Data?

While PII is a commonly recognized term, there is another term that many people may be familiar with — personal data.

The difference between PII and personal data can be explained by the following:

Personally Identifiable Information (PII) is a term used mainly within the USA.

Personal data is a term used in the EU's GDPR. Even though it is considered to be the European equivalent of PII, it doesn't completely correspond to the PII definition popular in the US.

Browser Settings

Although popular web browsers have long provided some level of privacy protection in the form of [DoNotTrack](#), few have implemented technical settings to strengthen user privacy when browsing the web.

But this has all changed over the past few years with the most popular web browsers by market share — Google Chrome, Mozilla's Firefox, and Apple's Safari — making gradual changes to how their web browsers handle cookies and other storage and tracking methods (e.g. device fingerprinting) to strengthen privacy for users.

Let's now take a look at how web browsers have strengthened user privacy and the impact these changes have had on digital advertising.

Apple's Safari

Apple's first real initiative to strengthen user privacy came in 2015 when they allowed iOS users to install content blockers (a form of ad blocking).

These content blockers can be downloaded from the App Store and used to prevent certain content (e.g. ads) and tracking cookies from loading in the Safari web browser on Apple smartphones and tablets.

Then, in September 2017, Apple stepped up their privacy game by introducing [Intelligent Tracking Prevention \(ITP\)](#) with the release of Safari 11 and iOS 11.

ITP is a feature of Webkit, an open-source web-browser engine that powers Apple's Safari web browser, that aims to further protect users' online privacy by changing the way Safari handles user identification methods, such as first- and third-party cookies.

The way ITP works is by classifying domains that are capable of tracking users across different domains via its Machine Learning Classifier.

Since its initial release, ITP has strengthened user privacy by limiting the lifespan of cookies and other data storage methods with every new update.

Here's an overview of the main restrictions ITP places on cookies and other browser storage methods as per ITP 2.3:

- Third-party cookies are blocked by default.
- First-party cookies created by JavaScript's Document.cookie API are set to expire in 7 days.
- First-party cookies created by JavaScript's Document.cookie API, classified as a tracking domain by the Machine Learning Classifier, and created via a link containing a query string or id fragment (known as link decoration) are set to expire in 24 hours.
- Data stored in local storage is set to expire in 7 days.
- All cookies created by a third-party CNAME-cloaked HTTP response will be set to expire in 7 days.
- In 2021, ITP will add a new feature that will hide a user's IP address from trackers.

How Does Intelligent Tracking Prevention Impact Digital Advertising?

The main problem companies in the digital advertising industry face when it comes to ITP is that it's harder to identify users across different websites.

The ability to identify a person across different websites is important for the following reasons:

- 1. Monetization for publishers:** The more a publisher knows about a visitor, the more ad revenue it will receive from advertisers, as we explain in the next point.
- 2. Revenue for advertisers:** Advertisers want to reach a specific audience, and if a member of that audience accesses a publisher's site, they'll likely submit a high bid in hopes their ad will be shown to them.
- 3. Relevance for users:** Although most people are uneasy with ads that follow them around the web, many users will click on or interact with ads if they are relevant to them; for example, an ad for a upcoming Metallica concert at CenturyLink Field would be of great interest to a heavy-metal fan living in Seattle.
- 4. Attribution:** One of the most overlooked areas of this whole identity problem is attribution. It's estimated that [global digital ad spend in 2019 will reach \\$316 billion](#), and without an accurate way to identify users as they move across the Internet and devices, it will be hard to track performance and know where to assign budgets.

In response to the limitations imposed on them by ITP, many AdTech companies have created workarounds, but these have either been eliminated or restricted with new releases of ITP.

Privacy Changes in iCloud+

Apple will introduce new privacy features that will be available to iCloud+ subscribers, which will be the paid iCloud subscriptions. The below changes won't be applied to the free iCloud subscriptions.

Private Relay

Private Relay encrypts the traffic between the Safari browser and the website a user is visiting. Nobody, including Apple or the network provider, can read the information being passed.

Here is Apple's explanation on how its [Private Relay works](#):

All the user's requests are then sent through two separate internet relays. The first assigns the user an anonymous IP address that maps to their region but not their actual location. The second decrypts the web address they want to visit and forwards them to their destination. This separation of information protects the user's privacy because no single entity can identify both who a user is and which sites they visit.

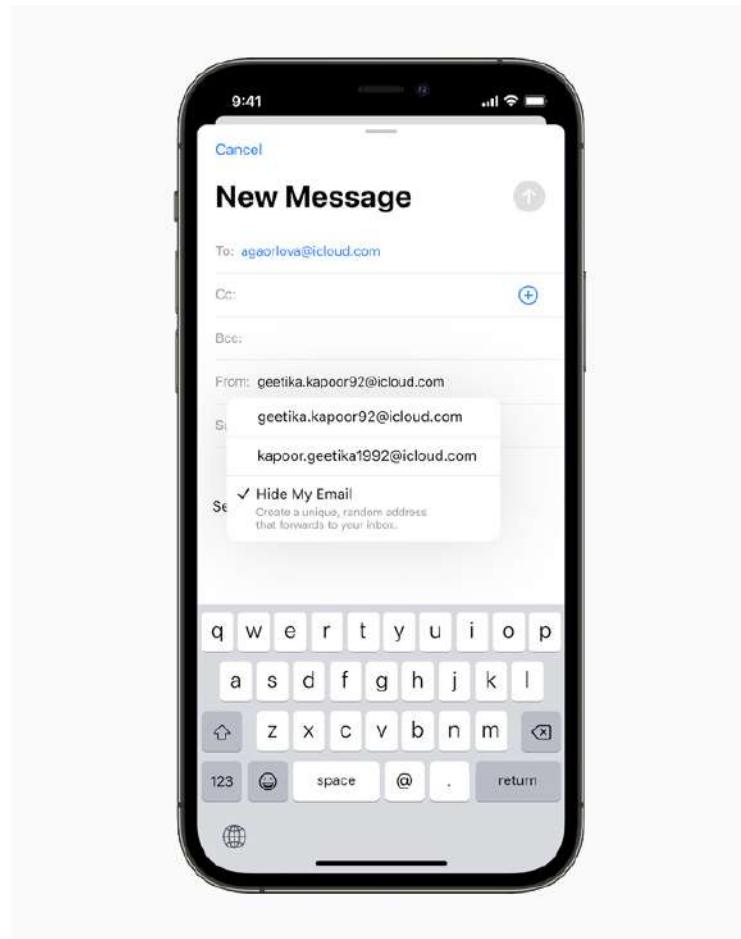
Mail Privacy Protection

This feature will prevent email senders from using invisible pixels to identify when a user opens an email. It will also mask a user's IP address so that it can't be used to determine their location or linked with other online activity.

Hide My Mail

The Hide My Mail feature will allow users to use a unique and randomly generated email address instead of using their actual email address.

The newly generated email address will forward to the user's personal email address and users can create and delete as many "hidden" email addresses as they like.



Source: [Apple](#)

The Impact of These Changes on Programmatic Advertising and AdTech

While these changes will increase user privacy, their impact on programmatic advertising and AdTech won't be as severe as some of the other privacy changes Apple has introduced.

Mail Privacy Protection will likely disrupt how email automation and MarTech tools work as they won't be able to report on open rates.

The Hide My Mail feature will throw a spanner in the works for ID graphs and ID solutions built around email addresses.

As these changes will only apply to iCloud+ subscriptions, not every Apple user will be covered by these changes.

According to a [group of Barclays analysts](#), Apple has around 850 million iCloud users, with about 170 million of those users on paid subscriptions, which accounts for 20% of all iCloud subscribers.

So around 170 million Apple users will see these new privacy changes come into effect when iCloud+ is released. The number of iCloud+ subscriptions makes up only 12% of [Apple's 1.4 billion active users](#).

Mozilla's Firefox

Firefox has also stepped up their privacy game by introducing Enhanced Tracking Protection (ETP) in June 2019 that blocked known trackers when browsing in private mode.

Then in September of the same year, Firefox released an update of ETP that blocks known third-party trackers as the default option for all Firefox users.

Apart from blocking known trackers, Firefox also blocks social media trackers, device fingerprints, and cryptominers.

Browser Privacy

Enhanced Tracking Protection



Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.

[Manage Exceptions...](#)

[Learn more](#)

Standard

Balanced for protection and performance. Pages will load normally.

Social media trackers

Cross-site tracking cookies

Tracking content in Private Windows

Cryptominers

Fingerprinters

Strict

Stronger protection, but may cause some sites or content to break.

Custom

Choose which trackers and scripts to block.

Google Chrome

Despite the fact that Google has a lot of skin in the digital advertising game with a large chunk of Google's revenue coming from ads and their own ad products, it has also made changes to improve the user experience and strengthen user privacy over the past few years.

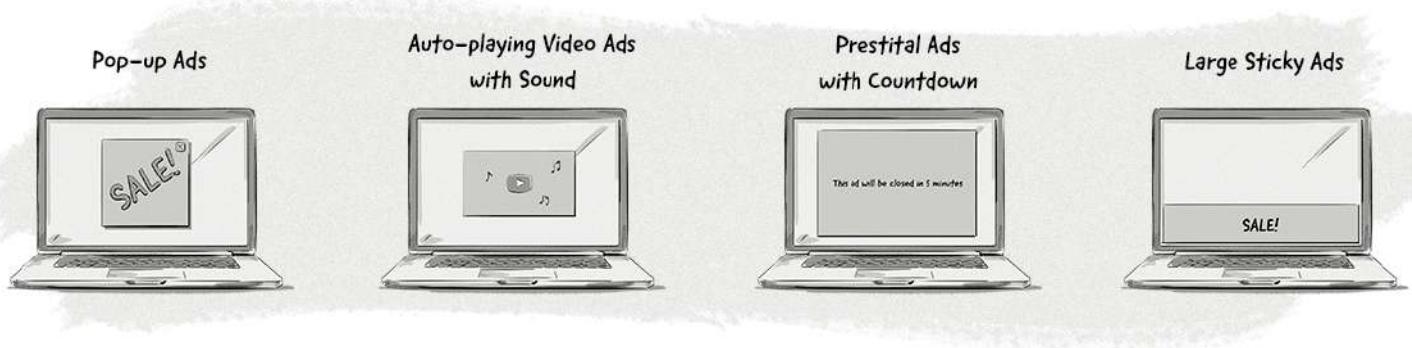
Chrome's Better Ads Standards

On February 15, 2018, Chrome released a built-in filter that blocks ads that don't comply with the [Better Ads Standards](#) proposed by the [Coalition for Better Ads](#) formed by leading associations and companies (including [Google](#) and [Facebook](#)). The coalition's goal is to improve consumers' experiences with online ads.

The filter does not get rid of ads completely (like a regular ad blocker), but protects the user from the most disruptive ads.

The filtered ads, according to www.betterads.org, include certain types of desktop ads:

- Pop-up ads
- Auto-playing videos with sound
- Prestitial ads with a countdown
- Large sticky ads



The types of mobile ad experiences least preferred by consumers and not complying by [Better Ads Standard](#) for ads on mobile devices include:

- Pop-up ads
- Prestitial ads
- Mobile pages with more than 30% ad density
- Flashing animations
- Poststitial ads that require a countdown to dismiss
- Full-screen scrollover ads
- Large sticky ads
- Auto-playing videos with sound



Pop-up ads



Prestitial ads



Mobile pages with more than 30% ad density



Flashing animations



Auto-playing videos with sound



Poststitial ads that require a countdown to dismiss



Full-screen scroller ads

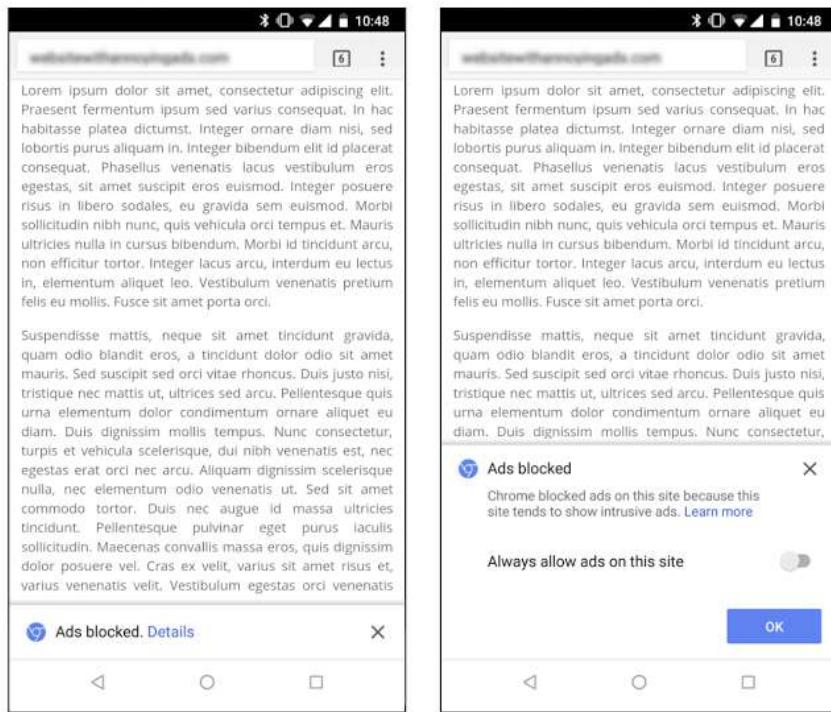


Large sticky ads

The Chrome filter is switched on by default and works in the following way:

- A Chrome user opens a new page.
- Chrome's ad filter first checks the page against a list of sites that notoriously fail the [Better Ads Standards](#).
- If the page is blacklisted, all requests for JavaScript ad tags or images ads will be blocked and won't be displayed. To determine which requests are ad-related, Chrome uses [EasyList patterns](#) used by most available ad blockers.

From an Internet user's perspective, when you open a website that is non-compliant with Better Ads Standards, you will see something like this:



Importantly, the filter doesn't block all the ads; only the intrusive, poorly designed ads that get on people's nerves the most. Ads that comply with [Better Ads Standards](#) will be displayed normally.

According to the standards proposed by the [Coalition for Better Ads](#), the following kinds of ads – unlike in the case of using an ad blocker like [Adblock Plus](#) – will not be blocked by the [Chrome](#) filter:

- Autoplay video ads (without sound)
- Skippable prestitials
- Ads that initiate up to 12 seconds of scroll lag to ensure you see them
- Flashing ads
- Side-rail takeover ads

Chrome's SameSite Cookies

On Wednesday, October 23, 2019, [Google Chrome released a detailed blog post](#) explaining changes about how cookies would be handled in the future.

The changes aim to give Chrome users more control over deleting third-party cookies, while keeping first-party cookies intact.

In short, website developers have to include a new "[SameSite](#)" attribute (specifically, SameSite=None) when setting a cookie to tell Chrome which cookies are to be used only by the current site or current URL that the user is on, and which ones are cross-site cookies.

Developers will also have to add the 'Secure' attribute as cookies will only be set via HTTPS.

Even though this attribute applies to Chrome, which was the first browser to support this attribute, it shouldn't cause any issues in other browsers that don't support it.

Setting cookies in this way will eventually help Chrome understand which ones are first party and which ones are third party.

In the future, Chrome could then ask users if they want to block third-party cookies. If the user says 'yes', then cookies created with `SameSite=None` will be blocked.

Chrome's Privacy Sandbox

On August 22, 2019, [Google announced a new initiative](#) that aims to make the web more privacy friendly, but still allows online advertising to work in a limited capacity.

This initiative is known as Privacy Sandbox.

Google is quick to reiterate that blocking third-party cookies completely without providing a solid alternative (like what Safari and Firefox have done) is detrimental to the future of the Internet (and the back pockets of publishers). It also acknowledges that users are demanding more control over their privacy.

Instead of blocking third-party cookies altogether, Privacy Sandbox provides a secure environment for personalization while still protecting user privacy.

Here are the key things to know about Privacy Sandbox:

- It's an open solution and Google has asked for feedback and input from other web browsers, publishers, and advertising technology (AdTech) companies on how to advance it.
- It is being positioned as a new web standard, rather than a new privacy feature.
- It will likely allow ads to still be relevant for users, but only anonymous and aggregated data would be available to AdTech companies and advertisers. Also, a lot more user data will stay on the device, instead of being passed on to AdTech companies.
- Google acknowledges that it can't go it alone and will require input and feedback from other companies and organizations.
- It's expected that Privacy Sandbox will go live in 2033.

Chrome's Plans to Kill Off Third-Party Cookies and the Move To Privacy Sandbox

On Tuesday the 14th of January, 2020, [Google made an announcement](#) that most people in the online advertising industry never thought they would hear — Google will kill off third-party cookies by 2022.

This announcement follows in the footsteps of their previous initiatives (listed above) and is the next step in Google Chrome's ongoing commitment to making the web a more privacy friendly place, while still allowing companies, including Google, to earn money from online advertising.

Here are the main things you need to know about this new announcement:

- Google Chrome plans to stop supporting third-party cookies by 2022.
- It will run a series of trials in 2020 to see how conversion measuring and personalization can work without using third-party cookies. This will involve using Privacy Sandbox (see above).
- The personalization element will probably be interest-based personalization on an aggregated level, rather than 1:1 personalization that has stood as the holy grail for advertisers and marketers for over a decade.

- The ultimate goal will be to replace third-party cookies used for ad selection and measurement with Privacy Sandbox.

As they've stated previously, Google doesn't see strict privacy features, like those seen by Safari and Firefox, as the way forward for the Internet and online advertising.

Google feels that these approaches only encourage companies to create workarounds and develop techniques like device fingerprinting, which further diminish user privacy and provide little or no control.

Just like with other sandboxes used in computer security, Chrome's Privacy Sandbox will execute advertising processes in a restricted environment, which is in stark contrast to how these processes are carried out today.

There are three parts to Privacy Sandbox:

- Replacing cross-site tracking processes — i.e. the ones currently powered by third-party cookies.
- Phasing out third-party cookies by separating first-party and third-party cookies via the SameSite attribute and turning off support for third-party cookies.
- Mitigating workarounds such as fingerprinting.

On Thursday June 24, 2021, Google Chrome announced that it would be extending its planned sunset of third-party cookies by 2 years. It's currently expected that Chrome will shut off support for third-party cookies starting from the middle of 2023.

Although it's still in development, Privacy Sandbox puts forward a completely new way of how online advertising works, particularly around **identification**, **ad targeting**, and **measurement**.

Identification in Privacy Sandbox

As part of its plans to improve user privacy, Privacy Sandbox won't identify individual users. This also means there probably won't be an ID that replaces cookies — i.e. no browser IDs.

This is the biggest change that the online advertising industry will have to get used to, as publishers, brands, agencies, and AdTech vendors have built their businesses around identifying individuals across the web via third-party cookies.

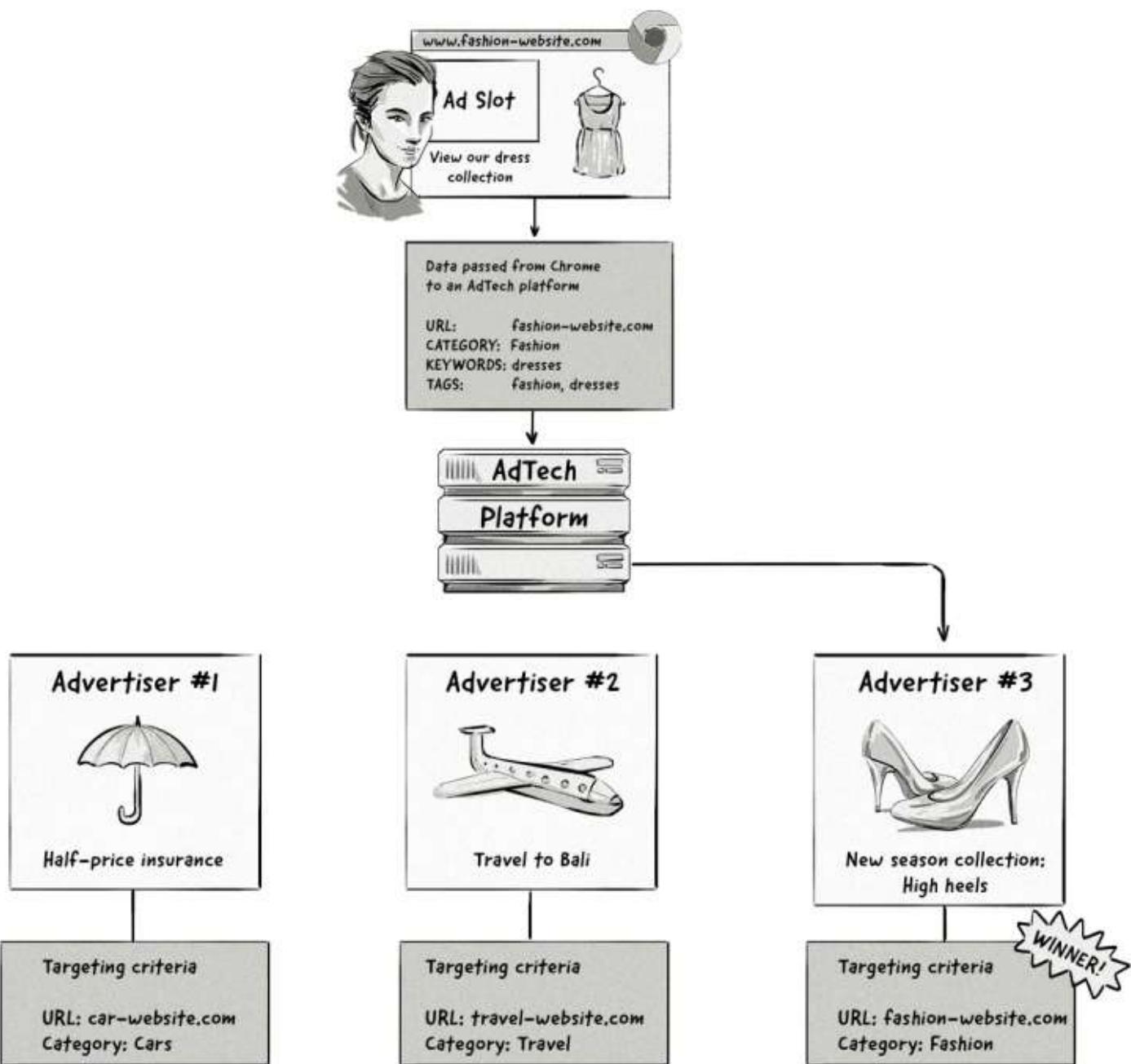
Although many AdTech vendors will turn to other identifiers such as first-party cookies, it's impossible to rule out the possibility of Chrome limiting the use of first-party cookies and other techniques for identification, like what Safari has done with Intelligent Tracking Prevention (ITP).

Ad Targeting in Privacy Sandbox

The ad-targeting options in Chrome's Privacy Sandbox will be fairly similar to the ones available today, but won't rely on user-level identification.

The main ad targeting processes in Privacy Sandbox are **contextual and first-party-data targeting**, **interest-based targeting via Federated Learning of Cohorts (FLoC)**, and **remarketing (aka retargeting)**.

Targeting method #1: Contextual and first-party data targeting

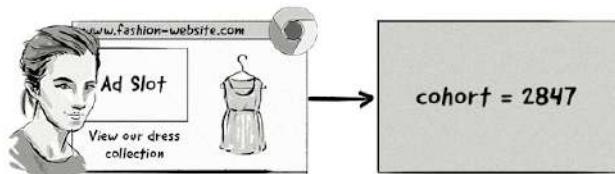


With this method, users will be displayed ads that match the context of the page they're visiting, similar to how contextual advertising works today.

The only difference is that Privacy Sandbox will be responsible for informing AdTech platforms about the context of the page, rather than the AdTech platforms themselves (e.g. via web crawlers and the user agent string).

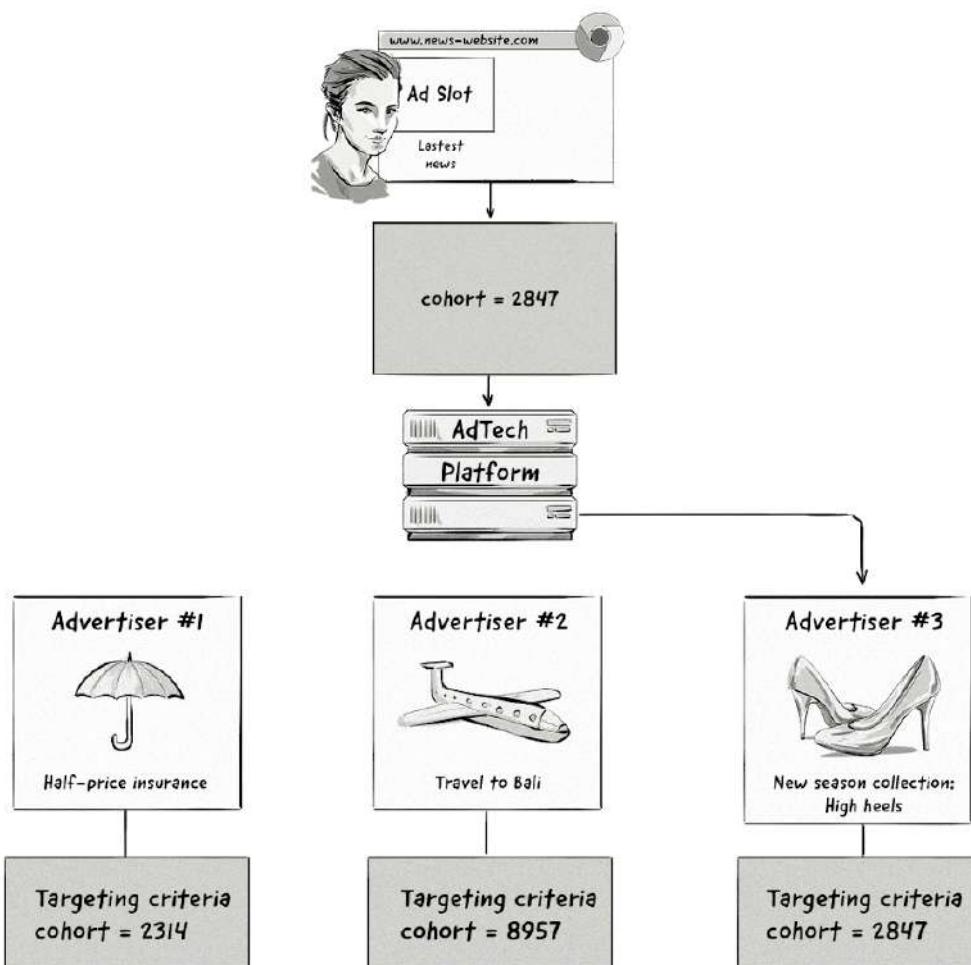
Interest-based ad targeting via FLoC

Phase #1: A user's web browser is added to a cohort based on their web-browsing history.



Phase #2: The user visits a different website. Chrome tells an AdTech platform (via the website) which cohort is associated with the browser.

Advertisers can show ads to users based on the cohort their web browser belongs to.



With interest-based targeting, a user will be added to a group based on the websites they visit. Advertisers will be able to target them based on the groups they belong to.

The important thing to note here is that targeting will be done on a cohort level, meaning no user data will be passed to AdTech platforms, just the name of the interest group they belong to. This new way of running targeted ad campaigns is in stark contrast to how it's done currently.

Google Chrome announced on January 25, 2021, that it would [make the FLoC API publicly available for testing](#) in March 2021, and begin testing FLoC in Google Ads in Q2 2021. These tests were released in most countries, except for countries in Europe as Google is not yet sure if FLoC complies with the GDPR.

Based on the tests Google's ad teams have conducted using FLoC, it claims that advertisers can expect to see **at least 95% of the conversions per dollar spent when compared to cookie-based advertising for reaching in-market and affinity Google Audiences.**

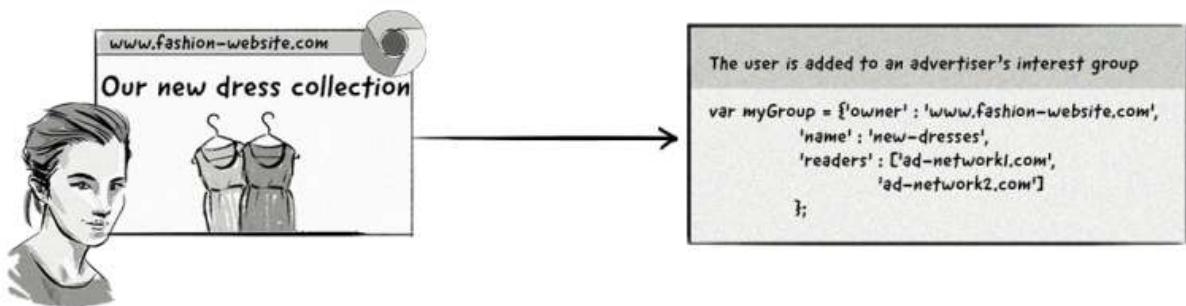
Then, on January 25, 2022, Google announced that it would be sunsetting FLoC and replacing it with a new initiative — **Topics API**.

Topics will enable advertisers to show ads to users based on the websites they visit, rather than the cohort they belong to. A classifier model will map website hostnames to topics and only subdomains and root domains will be included and not the full URL. For example, the website football.news.com will have the topic of football associated with it, but news.com/sport will have topics related to news.com associated with it.

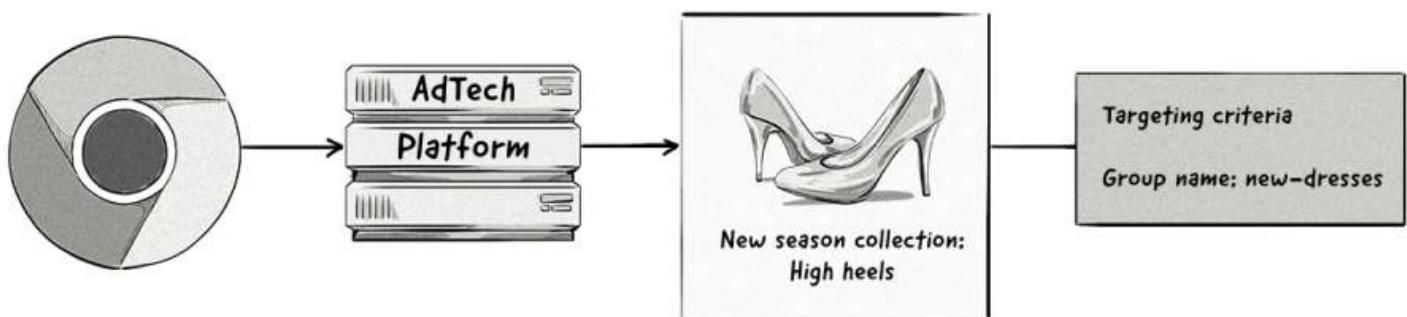
There are currently around 350 categories that will be included in the Topics API, but it's likely that this number will change.

Targeting method #3: Remarketing (aka retargeting)

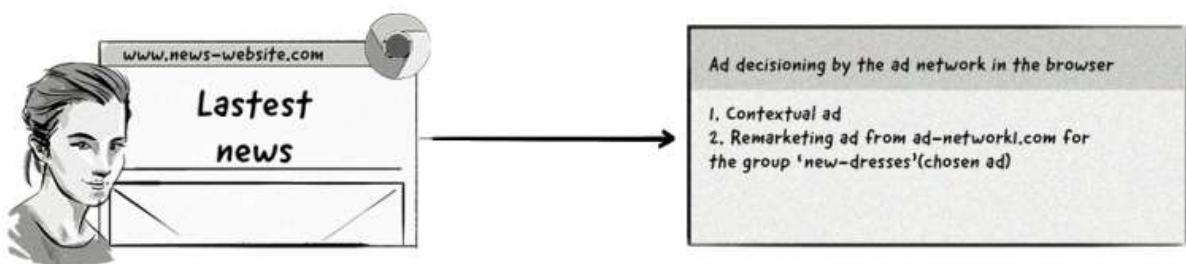
Phase #1: A user visits an advertiser's website and views a page displaying new dresses.



Phase #2: Chrome adds the user to ad-network1.com and requests ads for the group 'new-dresses'



Phase #3: When the user visits a different website that uses ad-network1.com, some code from ad-network1.com will load on the page and decide which ad should be displayed – i.e the contextual ad or the ad from the interest-based group.



The remarketing (aka retargeting) method is similar to the interest-based targeting method above, with the main difference being how the ad-decisioning process works.

With interest-based targeting, advertisers can show ads to users based on the interest groups they belong to.

With the remarketing method, the browser will send two ad requests to the AdTech platform — one containing contextual information and one referencing the interest group that the user belongs to.

The process Chrome's Privacy Sandbox will use for remarketing is known as Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE).

The AdTech platform won't know that these two ad requests are coming from the same user, hence the name 'two uncorrelated requests'. The reason for this is to make it hard for AdTech platforms to identify users by connecting the time the two requests are sent.

The interesting thing about this proposed approach is that many of the key ad-decisioning and even auction mechanics will be conducted client side (i.e. in the Chrome browser) instead of server side by AdTech platforms.

Other Proposals in Chrome's Privacy Sandbox

Apart from the standards mentioned above, there are many others that have been put forward by Google and other companies, including AdTech companies, advertisers, and publishers.

Some of these proposals include:

SPARROW: A proposal from Criteo in response to Chrome's TURTLEDOVE.

Dovekey: A follow-up proposal to Criteo's SPARROW from various teams at Google.

PARROT: A proposal from Magnite that's designed to maintain the privacy aspects of TURTLEDOVE but put control of the auction decisioning in hands of publishers by utilizing Fenced Frames (another proposal from the Google Chrome team).

TERN: a proposal from AdTech company NextRoll. The goal of TERN is to propose improvements to TURTLEDOVE based on information collected from GitHub issues and repos.

Fenced Frames: An API proposal created by Google engineers that would allow ads on a web page to load without the rest of the page knowing what ad is being displayed. The Fenced Frames API would be used to communicate with other Privacy Sandbox standards, like TURTLEDOVE, to show interest-based ads.

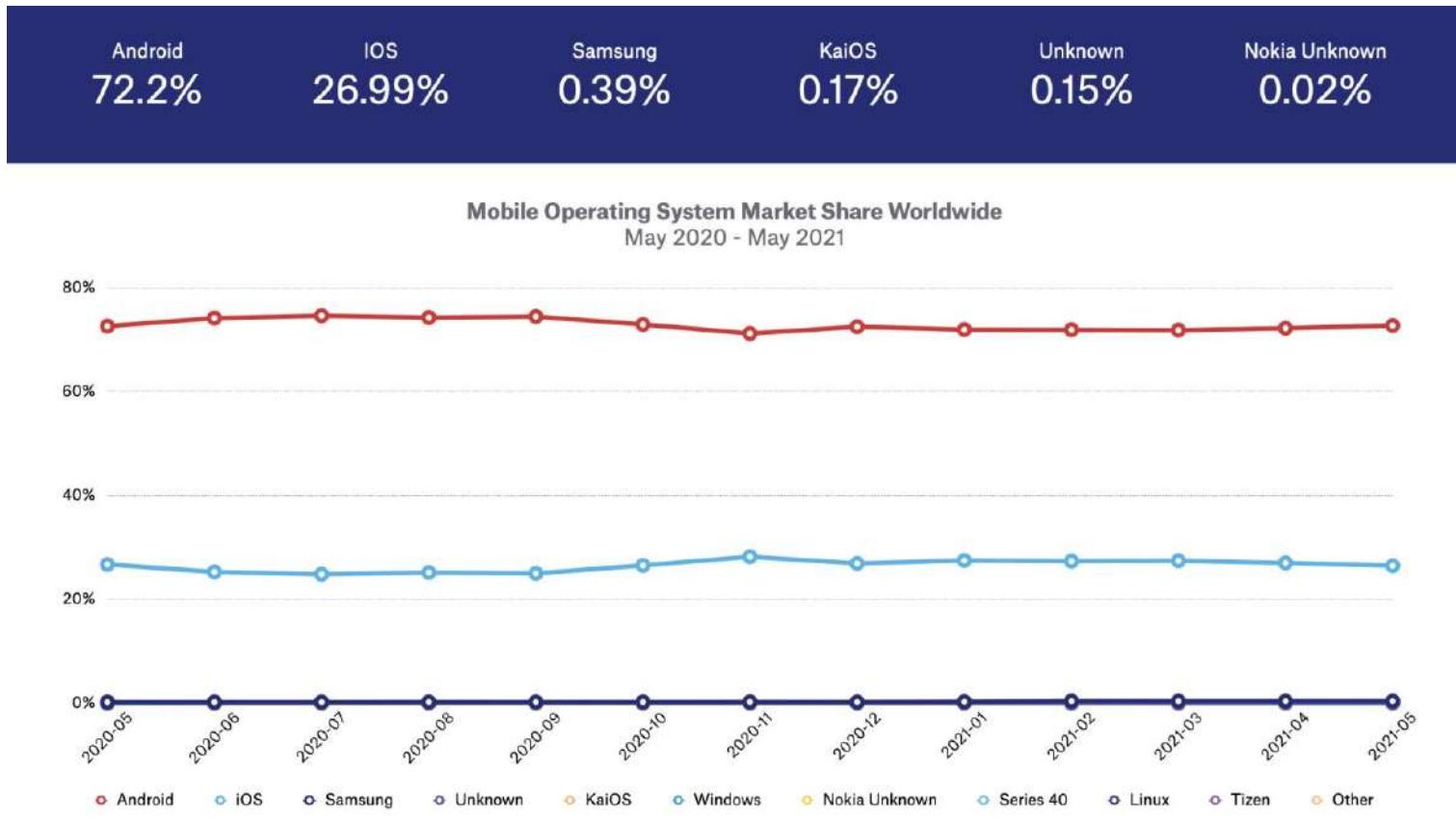
FLEDGE: A proposal from Google that's designed to be an early prototype of ad-serving processes in TURTLEDOVE. FLEDGE also incorporates components of the proposals made by independent AdTech companies (i.e. the ones listed above).

A full list of proposals can be found on the [W3C's Web Advertising Business Group Github repository](#).

Mobile IDs

Although most of the privacy changes over the past few years have been focused on web browsers, they are now starting to enter the in-app mobile world.

The two main mobile operating systems are Google's Android and Apple's iOS.



Source: [Statcounter](#)

Just like in the web-browser world, Apple has made a number of changes to iOS to increase user privacy over the past few years, including:

Limit Ad Tracking (LAT): An option that allows iOS users to opt out of targeted advertising. When enabled, the user's IDFA will be zeroed out (i.e. the random numbers and letters will be replaced with zeros) when accessed by apps and AdTech companies.

Opt out of location-based Apple Ads: This option allows iOS and macOS users to opt out of location-based ads served by Apple.

Grant or deny access to location data: The new release of iOS 13 brought with it an update to location data controls.

Firstly, users were periodically shown messages informing them of certain ads that were using their location data in the background (i.e. when not actually using the app in question).

Secondly, Apple presented users with a choice about whether an app could use their location data.

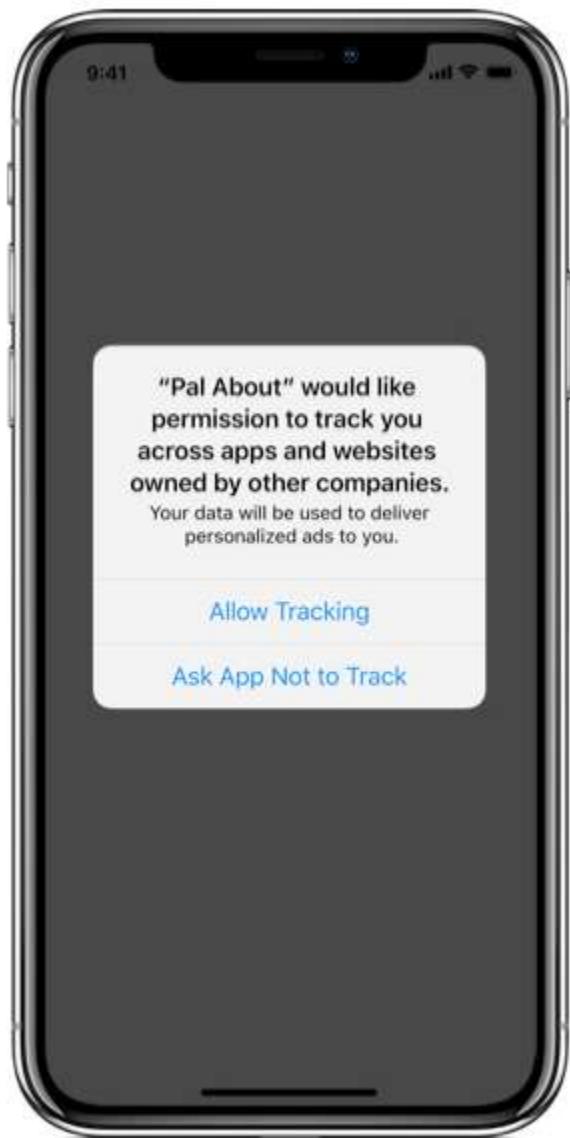
Apple's AppTrackingTransparency (ATT) Framework

During its Worldwide Developers Conference (WWDC), Apple announced that it would be introducing a series of privacy changes in iOS, iPadOS, and tvOS.

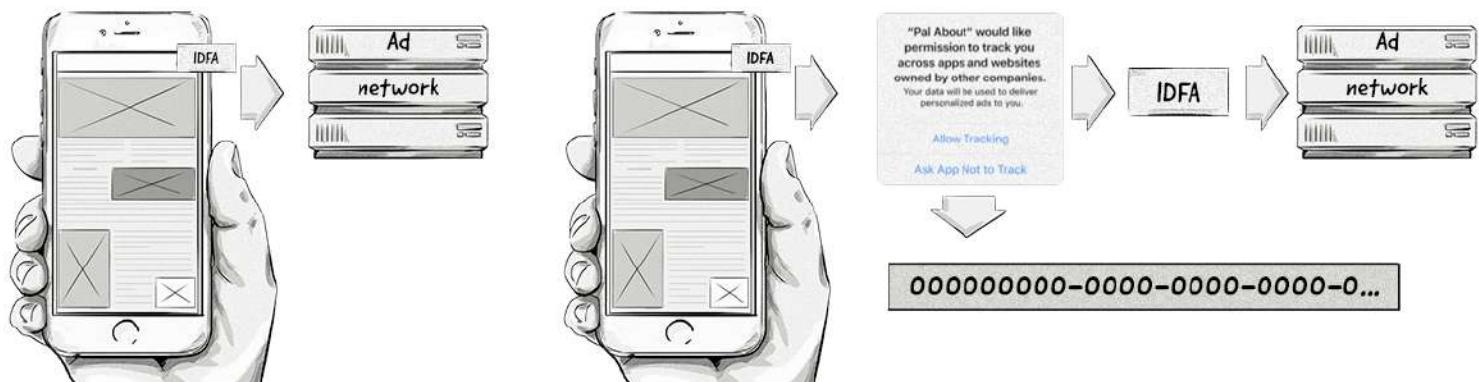
One of the main changes was to change how its mobile identifier (IDFA) is accessed by app developers, AdTech companies, and mobile measurement platforms (MMPs).

As of iOS 14.5, iPadOS 14.5, and tvOS 14.5, if app developers, AdTech companies, and MMPs want to collect a user's IDFA, they'll have to obtain consent via Apple's AppTrackingTransparency (ATT) Framework.

The framework involves showing users a message, similar to the one below, asking them if they can track them across different apps.



If users accept, then their IDFA will be collected. If they reject it, then the IDFA will still be collected but will be zeroed out, making it useless from an identification point of view.



The image on the left illustrates how the IDFA is accessed now.
The image on the right illustrates how the IDFA can be accessed in iOS 14.5

Apple's ATT framework has a very similar impact to the loss of third-party cookies in web browsers as it limits cross-app identification. In turn, this makes personalized ad targeting, retargeting, measurement, and attribution very limited.

Although Apple hasn't put forward a solution to ad targeting, it has released a solution for app install attribution via its SKAdNetwork.

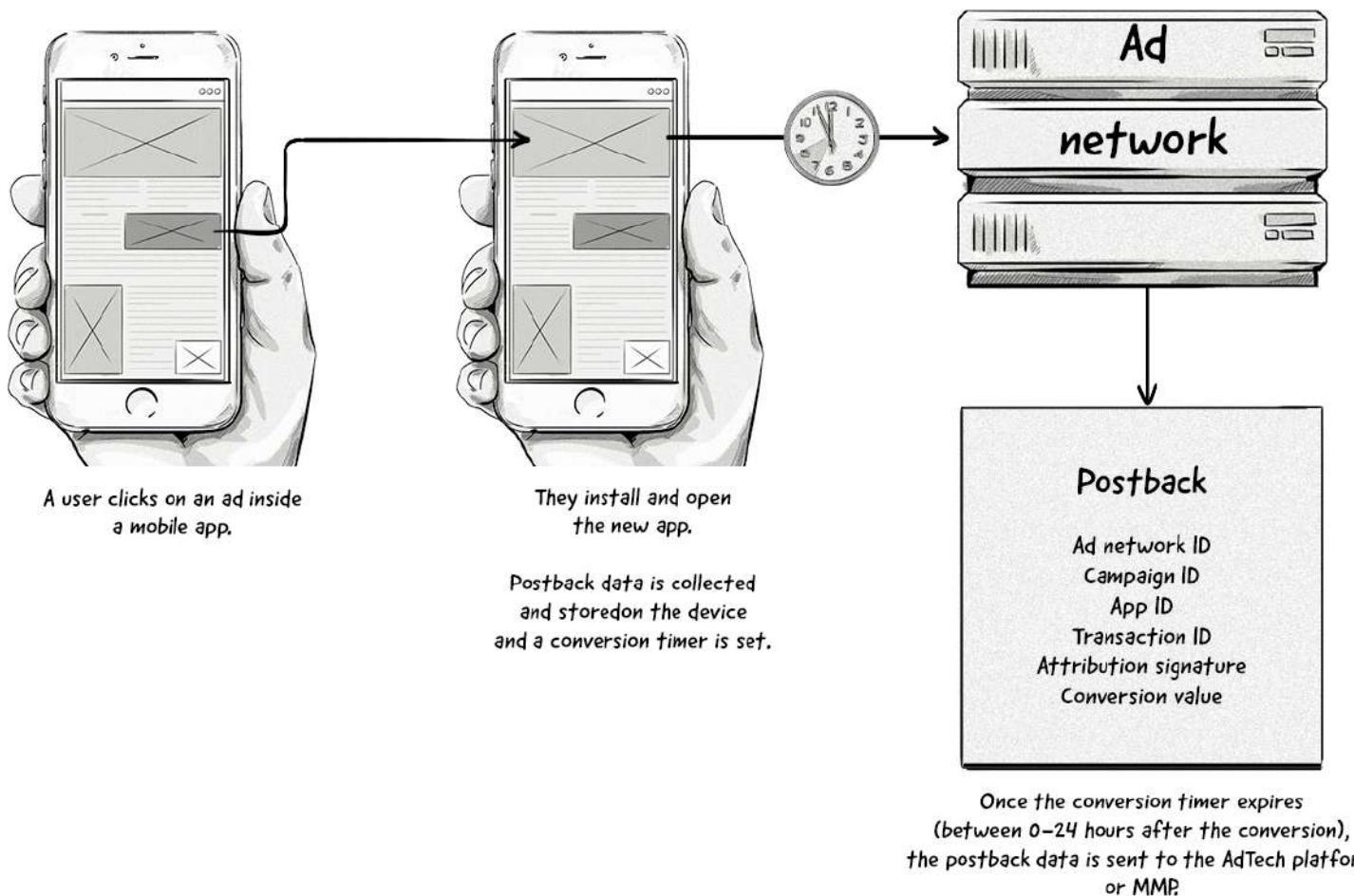
Apple's SKAdNetwork

Apple's SKAdNetwork aims to provide conversion data to advertisers but without revealing any user-level or device-level data. It's Apple's version of a privacy-friendly way to attribute app installs.

Here's how Apple's SKAdNetwork will work:

How Apple's SKAdNetwork API works

The SKAdNetwork is designed to attribute ad clicks with app installs in a privacy-friendly way.
No user-level or device-level data is passed to AdTech platforms or MMPs.



A couple of points about the SKAdNetwork:

- The IDFA won't be passed to AdTech platforms or MMPs, even if the user has opted in.
- All attribution data will pass through SKAdNetwork and then onto the AdTech platform or MMP. In iOS and iPadOS 15 onwards, advertisers will also be able to receive the postback information.
- SKAdNetwork will only attribute app installs (via the last-click model) and not view-through conversions.
- Campaign IDs are limited to 100 per AdTech platform (e.g. ad network or MMP).

Apple's Privacy Changes in iOS 15 and iPad 15

With the release of iOS 15, iPad 15, and watchOS 15, Apple will introduce a feature known as the App Privacy Report.

The App Privacy Report will give users more insights into how apps use things like their location, photos, camera, microphone, and contacts.

The report will show users how apps have accessed that information in the past 7 days and can deny access to that information by changing the settings.

The App Privacy Report will also show users which third-party domains the app has been contacting so that users can see which companies their data is potentially being shared with.

Google's Android Advertising ID (AAID)

Although Google hasn't announced any significant changes to its Android advertising ID (AAID), it has [hinted at making some changes in the future](#).

Google [recently announced](#) that it will require app developers to include privacy information in their Google Play Store listings, similar to the privacy information displayed in Apple's App Store listings.

Then in July 2021, Google announced that it would [stop passing on its AAID](#) if the user had opted out of personalized advertising. These changes went live with the release of Android 12 in the later part of 2021. While this is considered a privacy change, it's not as stringent as the ones released by Apple.

Ad Blockers

Ad blockers emerged in the mid-2000s and have risen in popularity over the past decade due in part to the growing concerns over user privacy and the pure annoyance of some ads (e.g. popup ads).

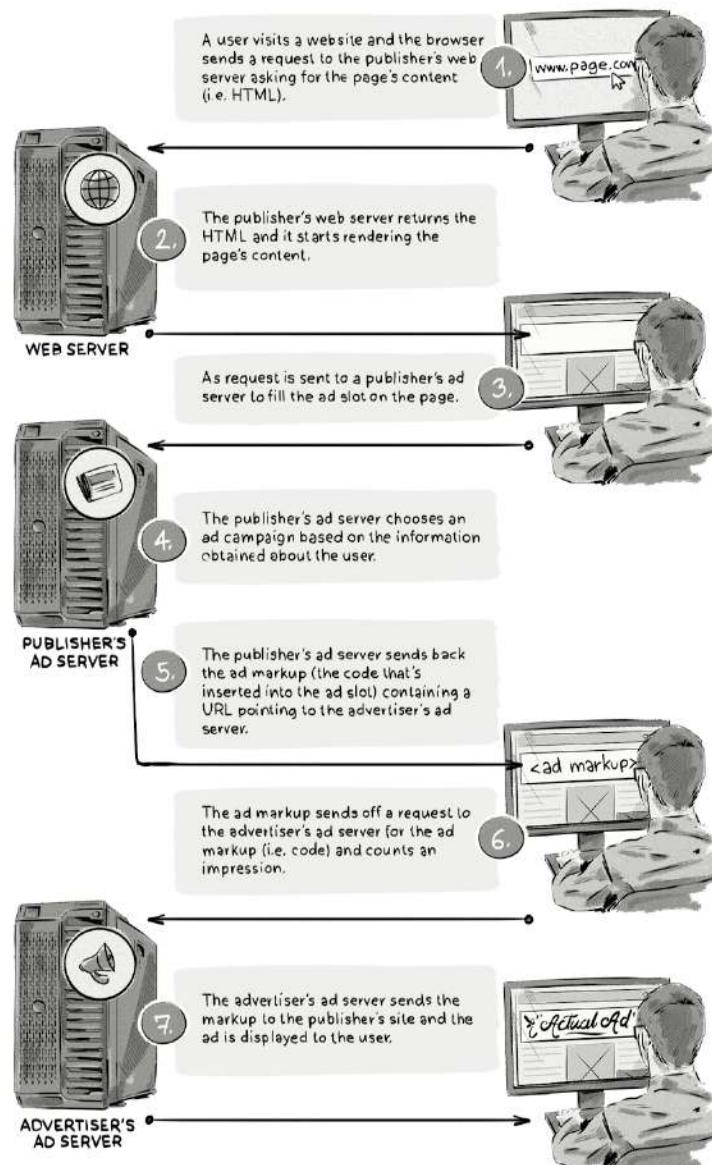
Although there are several ad-blocking methods, the most popular method by far is via web browser plugins like AdBlock Plus, Ghostery, and uBlock.

How Do Ad Blockers Work?

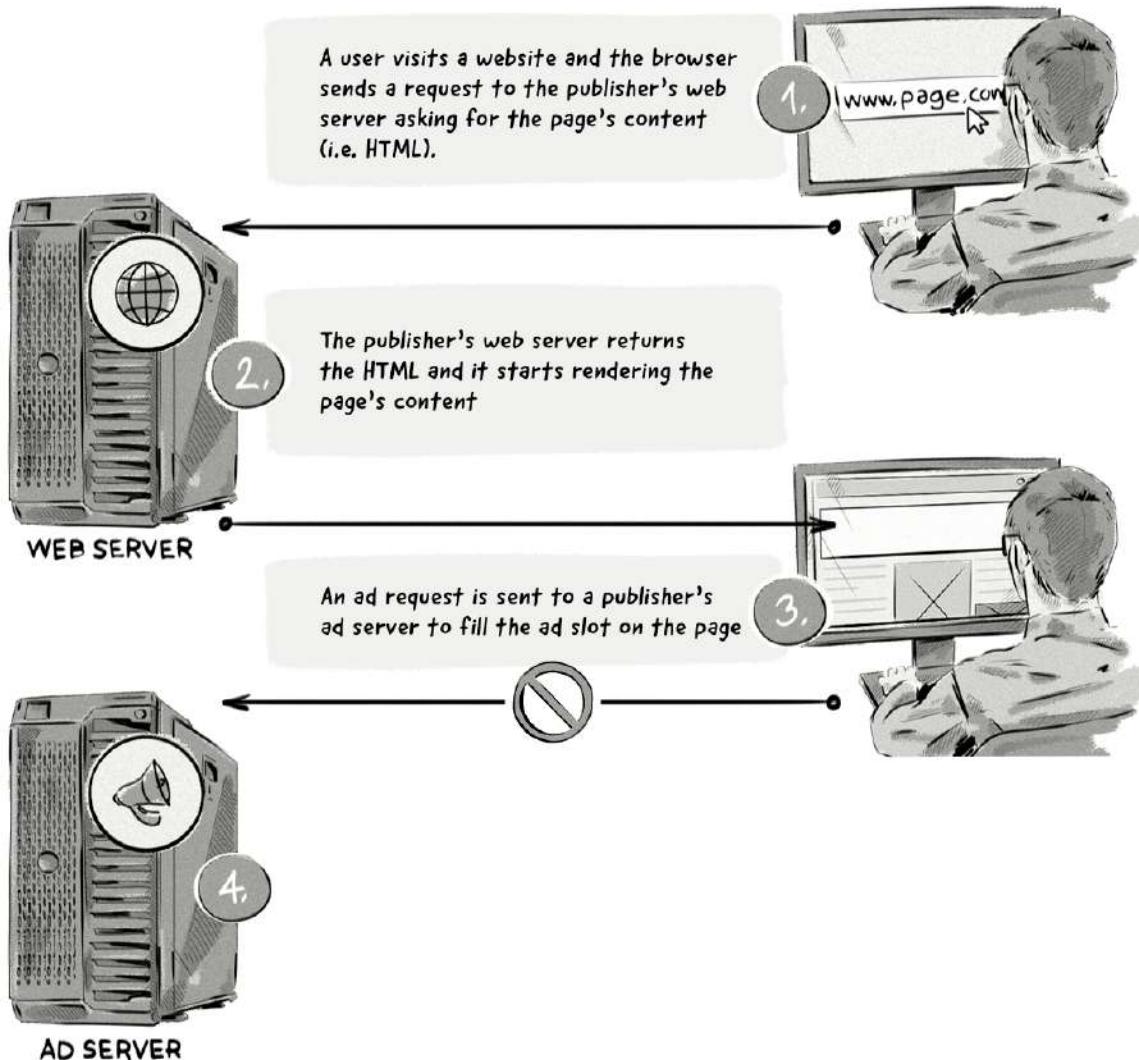
Most ad-blocking plugins work by preventing JavaScript and other elements from loading. This is achieved by adding domains used to serve ads to a blacklist and by identifying elements used for displaying ads, such as class="advertisement", class="banner_ad", and alt="ad" from loading.

Because most ad blockers stop AdTech JavaScript tags from loading, they not only stop ads from being displayed but also stop third-party cookies from being created. This means publishers miss out on ad revenue.

To highlight how ad blockers work, below we illustrate the normal ad-serving process where an ad is sent from an advertiser and displayed to a user on a website, and then how the process looks when an ad-blocking plugin is used.



And here's the same process but with an ad blocker:



Here's a step-by-step explanation of what's happening in the image above:

1. A user visits a website and the browser sends a request to the publisher's web server asking for the page's content.
2. The publisher's web server returns the HTML and it starts rendering the page's content.
3. The ad blocker extension scans the HTML, and:
 - A. Blocks the requests to load external resources, such as an ad request to the ad server domain (the ad request is not made).
 - B. Hides certain HTML elements from appearing, such as class="ad".

The Impact Ad Blockers Have On The Digital Advertising Industry

The impact of ad blockers on publishers is immediate, severe, and costly. It's estimated that ad blockers will [cost publishers \\$27 billion](#) in lost ad revenue in 2020.

According to [Growth of the Blocked Web 2020 PageFair Adblock Report by Blockthrough](#), over 615 million devices (desktop and mobile) worldwide have some sort of ad blocking software installed.

Desktop Adblock Users

Desktop adblock usage is slowly declining as users switch to mobile

- Despite slow decline, there were **236 million** monthly active users in Q4 2019.
- The frequency of use of desktop adblock software has begun to decline as users spend more time on their mobile devices.
- One drawback to replicating our methodology from past reports is that it omits adblockers not reliant on [EasyList](#). Though traditionally less common and difficult to account for, future reports will attempt to do so.



Mobile Adblock Users

More than twice as many people block ads on mobile web vs. desktop

- This growth is driven by mobile web browsers that block ads by default, especially in Asia.
- UC Browser is the most popular adblock browser. We estimate it has **405M** users worldwide.
- We estimate that Opera had **123M** mobile users in Dec 2019. Opera Mini now enables adblocking by default for new installations.
- The Brave adblock browser is growing fast in the US and Europe with **10.4M** users in Dec 2019 and **89% YoY growth**.



Source: [*Growth of the Blocked Web 2020 PageFair Adblock Report, Blockthrough.*](#)

What Can Publishers Do About Ad Blockers?

When it comes to addressing the issue of ad blockers, publishers first need to find out if a user is using ad-blocking software, and then use a variety of tactics to handle it.

How can publishers detect if someone is using an ad blocker?

Although it's difficult to bypass ad-blocking software, it's possible to determine whether someone is using an ad blocker by testing whether particular elements of the page have been displayed.

Typically, testing for the presence of an ad blocker involves adding a "bait" script — a tiny piece of code that an ad blocker is likely to interpret as an ad — to the publisher's website. This bait script could contain a class name like "banner_ad", which would likely be blocked by an ad blocker.

Examples of bait scripts and anti-ad-blocking scripts

Ad-block-detection scripts that are based on the aforementioned "bait" method take just a couple lines of code to implement. There are a few providers offering ready-made ad-block detecting scripts:

Detectadblock

[Detectadblock.com](#) proposes a method that requires a piece of JavaScript code to be saved. The method involves a hidden <div> section saved to a file called "ads.js", placed in the root directory of the website:

```
var e=document.createElement('div');
e.id='RZfrHsidDwbG';
e.style.display='none';
document.body.appendChild(e);
```

Publishers place the following JavaScript within their website's HTML source code just above the </body> tag. Its purpose is to check if the hidden DIV created within "ads.js" exists (ads are allowed) or not (ads are being blocked).

```
<script src="/ads.js" type="text/javascript"></script>
<script type="text/javascript">
if(document.getElementById('RZfrHsidDwbG')){
alert('Blocking Ads: No');
} else {
alert('Blocking Ads: Yes');
}
</script>
```

IAB Script

The Interactive Advertising Bureau (IAB), an advertising-business organization that develops industry standards, runs its own tech lab and has also proposed its own ad-block-detection script. It creates a set of "bait" DIVs likely to be blocked by browser-based ad-blocking tools. The script is really simple to set up, and

the IAB runs its own Github page (<https://github.com/InteractiveAdvertisingBureau/AdBlockDetection>) where you can find details about its inner workings.

BlockAdBlock

BlockAdBlock is a community-developed anti-ad-blocking script. Similar to the aforementioned methods, it's very simple and effective.

The bait used by BlockAdBlock looks like this:

```
baitClass: 'pub_300x250 pub_300x250m pub_728x90 text-ad textAd text_ad text_ads text-ads text-ad-links'
```

This means it will trigger ad-blocking software by referencing typical names and popular IAB-recommended ad-image sizes: 300x250px, 300x250px, and the skyscraper 728x90px. All these strings are referenced in Easylist. The script then detects whether the elements were displayed on the page.

How can publishers deal with ad blockers?

Detecting ad blockers is half the battle. Once a publisher determines that a user is using an ad blocker, they can then decide how to deal with it.

In March 2016, the IAB released its Publisher Ad-Blocking Primer, a 23-page document laying out seven tactics publishers can use to combat the ever-increasing ad-blocker problem.

The primer also includes a process known as DEAL, which the IAB suggests publishers follow when having conversations with visitors who use an ad blocker:

D

E

A

L

DETECT ad blocking, in order
to initiate a conversation

EXPLAIN the value exchange
that advertising enables

ASK for changed behavior in order
to maintain an equitable exchange

LIFT restrictions or **LIMIT** access
in response to consumer choices



The DEAL process and the Publisher Ad-Blocking Primer are just a few of the recent initiatives released by the IAB Tech Lab to combat ad blockers.

Others include the ad-blocking detection script (mentioned above) and the LEAN Ads Program, which aims to ensure ads complement and even enhance the user experience, rather than hinder it:



LIGHT

Limited file size with strict data-call guidelines

ENCRYPTED

Assure user security with https/SSL compliant ads

AD CHOICE SUPPORTED

All ads should support consumer privacy programs

NON-INVASIVE ADS

Ads that supplement the user experience and don't disrupt it

7 Tactics Publishers Can Use to Deal With Ad Blockers

The tactics provided by the IAB cover a range of possible implementations and can be used separately or in conjunction with others.

All of the seven recommendations listed by the IAB come with their own risks and benefits. The IAB suggests publishers weigh up the risks and benefits and consider the type of relationship they have with their audience before deploying a tactic.

Here's a brief recap of the items mentioned in the Publisher Ad-Blocking Primer and some examples of what they look like in action.

1. Notice

This tactic involves publishers detecting an ad blocker and then taking one or more of the following actions:

Educating and informing the user about the negative implications of ad blockers and the value of advertising (e.g. free content in exchange for viewing an ad).

Requesting the user disable the ad-blocking software in order to continue.

Asking the user to donate money to avoid seeing ads.

Telling the user that if they want to use an ad blocker, their experience will be limited.

The aim of the Notice tactic isn't necessarily to force the user to disable their ad blocker, but to start a conversation regarding their ad-blocking choices and encourage them to take a certain action. The Guardian is just one publisher out of many using the Notice tactic:



We notice you're using an ad-blocker. Perhaps you'll support us another way? Become a Supporter for less than \$1/€1 per week

2. Access Denial

Access denial goes one step further by restricting access to the site (or parts of the site) until the user has completed an action proposed by the publisher — e.g. switching the ad blocker off, subscribing, registering, or making a donation.

An example of the Access Denial tactic can be found on Forbes:



3. Tiered Experience

Unlike the above tactic that denies the user access to content, the tiered experience method works by delivering a limited or modified experience to a user who has an ad blocker installed while delivering the full experience to a user who doesn't.

For example, a publisher may only allow users with an enabled ad blocker to read five articles per month, but let users without ad blockers read a higher or unlimited number of articles.

This tactic is similar to paywalls publishers use to encourage visitors to take out a paid subscription:

10 free articles a month go quickly.
Dive in, and continue enjoying The New York Times.
[Get 60% off for one year.](#)

Limited time offer. You may cancel anytime.

Source: *The New York Times*

Subscribe now for full access or register to continue reading.

You have reached your article limit

Source: *The Economist*

4. Payment From Visitors

The payment from visitors tactic can relate to both monetary and non-monetary payments.

For example, a publisher may ask the visitor to pay a small fee to access the content or provide their email address.

Examples include:

Subscription: A visitor pays or provides some information (e.g. a name and email address) for continued access to the content, just like in the example below from bild.de.

Punch-Card: A visitor pays for a set number of accesses (e.g. \$10 for 10 articles).

Timed Pass: A visitor pays for access for a limited period of time (e.g. \$10 for one month).

Members-Only Section: A visitor pays for access to content or features only available to paying members.



With Adblocker activated, you can no longer visit BILD.de

disable Adblocker Now

or [subscribe image Smart](#)

5. Ad Reinsertion

Publishers can also resort to ad reinsertion, which is arguably the least ethical and user-friendly way to fight ad blockers.

The term describes the practice of finding ways to serve ads to users that have an ad blocker installed. Ad reinsertion may be done with or without the permission of the adblock software provider.

While this technique may actually stop ads from being blocked (at least for some time), actual short-term and long-term implications of ad reinsertion are still unknown—in fact it's advertising to people who explicitly don't want to be advertised to.

The method is a constant cat-and-mouse game that may involve a lot of effort on the publisher's side, but ultimately bring little benefit.

Ad reinsertion is comprised of three main methods:

Obfuscation: This method attempts to avoid ad-blocking software by changing the names of the ads and their location on the page.

In browser: Similar to above, this method aims to avoid being picked up by ad blockers by using software in the browser to change the requests sent to the ad resources.

On server: Using a process known as server-side ad stitching (a.k.a. ad insertion or dynamic ad insertion), this method delivers the ad from the same server as the content or service, which avoids detection from ad blockers.

6. Payment to Ad Blocker Companies

All of the aforementioned tactics relate to technology solutions, whereas this is more of a business solution to the ad-blocker problem. Payment to ad blocker companies involves buying your way onto ad-blocker whitelists so your ads are not blocked by the software.

Adblock Plus (ABP), one of the most popular ad blockers, has created a program called Acceptable Ads Program, in which companies can apply to its whitelist so their ads can still run even if the ABP software is active.

Here's a snapshot of ABP's whitelist:

```
! Amazon text ads
(https://adblockplus.org/forum/viewtopic.php?f=12&t=9791)
@@|amazon.com^$elemhide
@@|amazon.ca^$elemhide
@@|amazon.de^$elemhide
@@|amazon.co.uk^$elemhide
@@|amazon.fr^$elemhide
@@|amazon.es^$elemhide
@@|amazon.it^$elemhide
@@|amazon.co.jp^$elemhide
@@|amazon.cn^$elemhide
@@|amazon.com.au^$elemhide
@@|amazon.com.br^$elemhide
@@|amazon.in^$elemhide
@@|amazon.com.mx^$elemhide
@@|amazon.nl^$elemhide
@@|d14qd3he45186l.cloudfront.net/ads-
search*.html$subdocument,document,domain=amazon.com|amazon.ca|
amazon.de|amazon.co.uk|amazon.fr|amazon.es|amazon.it|amazon.co
.jp|amazon.cn|amazon.com.au|amazon.com.br|amazon.in|amazon.com
.mx|amazon.nl
```

In the image above, you can see that Amazon ads are on the whitelist, which means they should still appear even if the ABP software is active.

7. Payment to Visitors

Similar to the previous strategy, this one involves paying or rewarding visitors for their time spent with advertising. Examples of this include sharing a portion of ad revenue with users and giving them extra playing time if they view ads on a mobile game.

8. Native Ads

Another effective way to circumvent ad-blocking software is to display native ads.

Native ads are inherently more difficult to detect, as the ad content is implemented in such a way to largely resemble the original content on the website.

Native in-feed ads match the original editorial content in form and function, making them difficult to detect.

This is a very effective way to monetize content, and is used by some of the biggest players in the industry, including [Facebook](#), [LinkedIn](#), [Tumblr](#), [Twitter](#), and [Instagram](#). Major news media—including [Time](#), [Forbes](#), [The Wall Street Journal](#), and [The New York Times](#), quickly sensed potential and jumped on the native bandwagon.

However, because most native ads are served via third-party AdTech platforms and contain similar elements to banner ads (e.g. class="native-ad"), there's still a chance that they'll be detected and blocked.

Opting Out Of Online Behavioral Advertising

Online behavioral advertising (OBA) simply means targeting online consumers with ads that align with their online behavior — typically, what types of websites they visit.

So for example, if you regularly visit websites about cooking, you will more than likely see ads about cooking, such as kitchen products and cookbooks.

Behavioral targeting helps advertisers display ads that are relevant to your needs and interests. However, some consumers wish not to receive these types of ads as they don't like the fact that companies collect information about them.

How can Internet users opt-out of behavioral or targeted online advertising?

There are 4 main ways online users can opt-out of behavioral or targeted advertising.

Solution # 1: Unchecking the opt-in option found on a web page.

OPT OUT

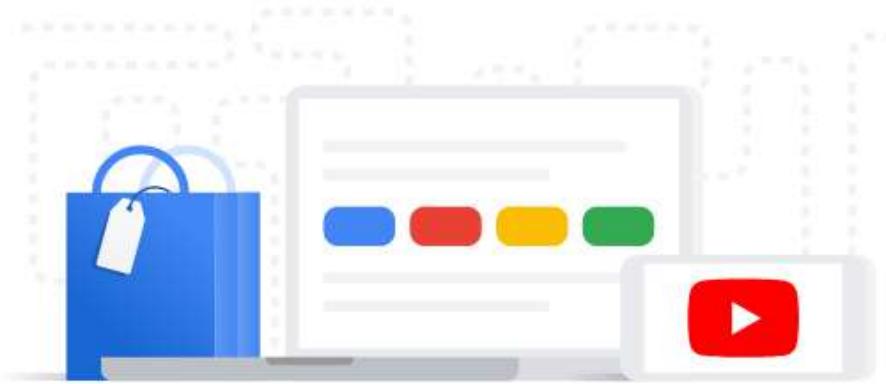
You can choose to opt out of being tracked by all marketing and advertising tools installed on this website. To make that choice, please click below to receive an opt-out cookie.

You are currently opted in. [Click here to opt out.](#)

Some websites include an option for you to opt-out of marketing for that site. It's important to note that by doing so, you are only opting out of this particular site and it won't opt you out of other sites.

When a user opts out or a particular site, a cookie is set in the first-party cookie of the publisher. This cookie is then checked, typically by a tag manager, before any tags get served. If the opt-out cookie is detected, the tags aren't fired.

Solution #2: Turning off the personalization feature on popular search engines (i.e. Google, Bing, Yahoo!) and other sites (e.g. Amazon and Facebook).



Ad personalization

Google makes your ads more useful on Google services (such as Search or YouTube).

Ad personalization is ON

Control ad personalization on other websites & apps that use Google ad services.

You can not only opt out of behavioral targeting but can also change the settings in your web browser so that you are displayed ads that are more relevant and of interest to you.

If you turn this option off, then you will still see ads, but they will be general and location-based ones, rather than ones that match your interests.

When a user opts out from search engines and accounts, the opt-out request is set at the account level, rather than saved as a first-party cookie. So when you're logged in to the site, the website (e.g. Facebook, Google, Amazon, etc.) knows that you have opted out and therefore doesn't personalize the ads or pass additional information about you to the ad platforms.

However, this method of opting out does not prevent these companies from collecting data about your behavior; it just means they won't use data collected about you for ad personalization.

Solution #3: Requesting AdTech vendors and their clients to not track you across their products.

We understand if you wish to opt out of LiveRamp

Our Opt-out Tools

[Opt Out of Cookies >](#)

[Mobile Opt-Out >](#)

[Permanent Opt-Out >](#)

[Data Plus Math Opt-Out >](#)

[Arbor Opt-Out >](#)

You may also want to change the cookie management settings on your web browser.

- To manage advertising cookies used by your web browser, visit the opt-out page from the DAA's [AboutAds](#) site. Cookies placed by LiveRamp are those under the company names *LiveRamp* and *Arbor* in the AboutAds company list.
- To opt out of records other than cookies and mobile device IDs, please utilize the email opt-out described below.

The example above is from LiveRamp, which is a company that provides data to advertisers and AdTech companies.

This is a similar process to the first point, however, opting out of the Ad Tech & MarTech products will apply to all websites that use that particular software or platform.

This method works in a similar way to the first solution, except instead of creating a first-party opt-out cookie on the publisher's side, a third-party opt-out cookie is created on the AdTech vendor's side. Organizations like the NAI (mentioned below) allow users to opt out of behavioral targeting from all the members (i.e. vendors) in their organization.

The third-party cookie's value is then sent with every request to the participating vendors advising them that the user has opted out and therefore shouldn't apply behavioral targeting in ads or collect behavioural data.

While this method allows users to opt out from multiple companies at once, it's up to vendors as to whether they respect the user's decision to opt out or not, but since it's their opt-out cookie, they generally should uphold the user's decision.

Solution #4: Opt out of behavioral advertising via Advertising Organizations

There are a couple organizations that exist to help online users control how their data is collected and used for activities such as behavioral targeting.

The two main organizations are the **Network Advertising Initiative (NAI)** and the **Digital Advertising Alliance (DAA)**.



The **Network Advertising Initiative (NAI)** is the leading self-regulatory association consisting of third-party digital advertising companies.

The **NAI** is a non-profit organization and aims to promote the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for advertising online and in mobile.

The NAI provides a tool that allows online users to opt out of behavioral advertising.

The NAI opt-out tool:

- Only affects behavioral advertising.
- Opts users out of behavioral targeting from NAI members only.
- Doesn't delete cookies nor remove online ads completely.
- Allows users to choose which companies to opt-out of.
- Sets an opt-out cookie in the user's browser for each of the companies the user selects.

OPT OUT OF INTEREST-BASED ADVERTISING

Welcome to the NAI's opt-out page where you can learn more about NAI members who deliver tailored online ads and your choices to opt-out of receiving them. To learn more about this tool and how it works, please scroll down to read More Info.

[Manage My Browser's Opt Outs](#) 

Select "Manage My Browser's Opt Outs" to see which participating NAI members may be engaging in Interest-Based Advertising on this browser and to choose which members' IBA activities you wish to opt out of.

[Learn About Mobile Device Opt Outs](#) 

Select "Learn About Mobile Device Opt Outs" to learn more about Cross-App Advertising and to opt your device out of receiving ads tailored to your interests.

Source: <http://optout.networkadvertising.org/>



The Digital Advertising Alliance (DAA) is an independent non-profit organization led by leading advertising and marketing trade associations.

The purpose of the DAA is to establish and enforce responsible privacy practices across the digital advertising industry to provide consumers with enhanced transparency and control.

The DAA is the organization behind the **YourAdChoices** initiative, which is represented by the icon (in the DAA logo above) on some display ads.

Through its YourAdChoices initiative, the DAA offers a browser tool, known as WebChoices Tool, that allows online users to opt out of behavioral targeting from DAA's participating companies.

Company	Customizing Ads on your Browser	Opt Out? select all
33Across	Status Unavailable	<input type="checkbox"/>
4 Info	Status Unavailable	<input type="checkbox"/>
<intent>	Status Unavailable	<input type="checkbox"/>
AcuityAds	Status Unavailable	<input type="checkbox"/>
Adara	Status Unavailable	<input type="checkbox"/>
Adbrain	Status Unavailable	<input type="checkbox"/>
AddThis	Status Unavailable	<input type="checkbox"/>
Adelphic	Status Unavailable	<input type="checkbox"/>
Adform	Status Unavailable	<input type="checkbox"/>
AdGear Technologies	Status Unavailable	<input type="checkbox"/>
Adobe Marketing Cloud - Advertising Services	Status Unavailable	<input type="checkbox"/>

UNDERSTAND YOUR CHOICES

OPT OUT OF ALL

SUBMIT YOUR CHOICES

Submitting your choices for all currently participating companies stores your opt out preferences in your browser. [Learn More.](#)

Just like with the NAI opt-out solution, if a user deletes their cookies, then they will have to go through the opt-out process again.

Solution #5: Disabling third-party cookies from being saved in your web browser and activating the Do-Not-Track feature.

Standard

Balanced for protection and performance. Pages will load normally.

Social media trackers

Cross-site tracking cookies

Tracking content in Private Windows

Cryptominers

Fingerprinters

Strict

Stronger protection, but may cause some sites or content to break.

Custom

Choose which trackers and scripts to block.

Send websites a "Do Not Track" signal that you don't want to be tracked [Learn more](#)

Always

Only when Firefox is set to block known trackers

You can disable third-party cookie tracking and enable the Do Not Track option in your web browser by adjusting the privacy preferences in the web browser's settings.

The **Do Not Track (DNT)** option requests that a web application disable either its tracking or cross-site user tracking of an individual user.

The DNT header is automatically attached with every HTTP request that the user's browser makes, but it's up to the vendor receiving the request (e.g. ad server, SSP etc.) to honour it or not.

Apple's Safari no longer supports DNT as it provides little protection over a user's online privacy.

The Implications Of Opt-Out Solutions

There are 2 main implications opt-out solutions have on the online advertising industry:

1. Lower ROI for advertisers.

The implications of opt-out solutions affects both the advertiser and publisher because if more and more users decide to opt out of behavioral advertising, then this will devalue the publisher's audiences & traffic and will cause their inventory to be less valuable.

For advertisers, their ROI will be impacted as their ads won't be shown to engaged or interested users.

2. Lower revenue for publishers and less opportunities to monetize the Internet.

Currently, publishers and app developers display ads as a way to monetize their content and apps, most of which are provided for free. The increase in opt outs will result in publishers and app developers charging for their content and apps.

There are quite a few publishers, mainly large news sites, that already charge for their content, but this type of monetization model could increase. Similarly, app developers could start charging for their apps, which could lead to a decrease in free apps available to users.

Differing Views on Data Collection

There are many different views and opinions on the way users' data is collected, shared, and sold online.

Some believe that if the tracking is only for advertising purposes, it poses no great risk to their privacy, while others believe that it is a clear violation of their privacy and will go out of their way to prevent companies from tracking their online movements.

Online privacy is a hot topic, especially since the [NSA scandal broke in 2013](#), and with more and more users going online, the opportunities for companies to target them with their ads is only going to increase.

But regardless of your own view on data collection, it is an area of online display advertising that has many challenges to overcome, both from the business side and from the user side.

Online Ads And Their Common Pitfalls Of The User Experience

Apart from the privacy concerns users have about online ads, many also feel the user experience is disrupted by ads.

A [2017 report by PageFair](#) uncovered some of the reasons why online users implemented ad blocker software.

Adblock user motivations

People use adblock for many, diverse reasons.

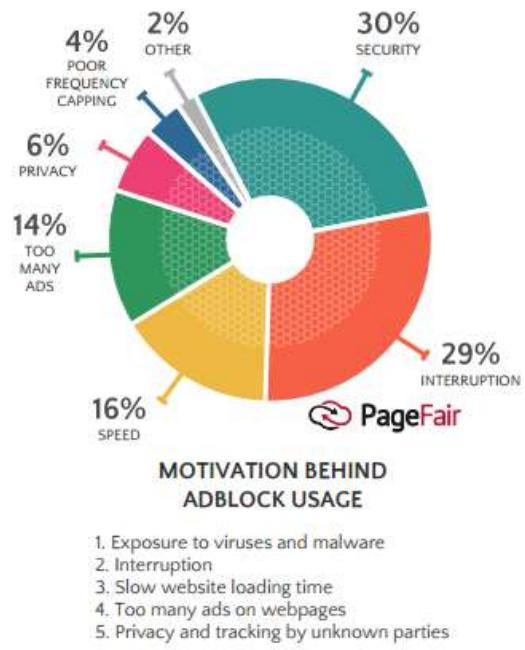
Key findings

- **Interruptive ad formats and virus/malware concerns** were the leading reasons given for adblock usage.
- **38%** more women than men indicated concerns about viruses and malware as their main motivation.
- **14%** more men than women stated that interruption was their top concern.
- Over **70%** of users chose more than one reason as "most important" in their choice to use adblock software.
- Outside of security and interruption, user motivation did not vary significantly by demographic segment.
- While privacy was a top concern for early adopters of adblock software, it is less so for a mainstream audience.

Conclusion

Adblock usage is driven by specific problems with the delivery of online advertising, and is not a rejection of digital advertising itself.

PAGEFAIR | 2017 Adblock Report



1. Exposure to viruses and malware
2. Interruption
3. Slow website loading time
4. Too many ads on webpages
5. Privacy and tracking by unknown parties

PageFair

Source: [The state of the blocked web, 2017 Global Adblock Report, PageFair, 2017.](#)

Below is a detailed explanation of some of the common pitfalls of online ads.

Too Many or Annoying Ads

One of the main reasons why users install ad blockers is because they are shown too many ads, which often has a negative impact on the user experience.

12

The screenshot shows the Cambridge Dictionary homepage. At the top, there are links for Dictionary, Translate, Grammar, and Cambridge Dictionary +Plus. On the right, there are social media icons for Facebook, Instagram, Twitter, and a 'Log in / Sign up' button. Below the header, there's a search bar with 'Search English' and a dropdown menu set to 'English'. To the right of the search bar are links for Grammar, English-Spanish, and Spanish-English. A decorative banner for Disney+ and Star Wars: The Mandalorian is displayed. The main content area features a large advertisement for 'advertising' with a definition, examples, and a 'Try a quiz now' button. To the left, there's a sidebar for 'Premium speed. Unlimited data.' with a 'Find out more' link. The bottom of the page includes a footer with legal text and a copyright notice.

This webpage has **3 ads** above the fold (the top visible area of the page).

In addition to traditional banner ads, many websites also have pop-up ups, which are considered the most annoying type of ad as they tend to take up the whole page, stop the user from doing what they were doing (e.g. reading an article), and often require the user to click a small cross to close the ad.

Adware

Adware is a form of software that downloads or displays unwanted ads when a user is online, collects marketing data and other information without the user's knowledge or redirects search requests to certain advertising websites.

Adware that does not notify the user and attains his or her consent is regarded as malicious.

Adware is the name given to programs that are designed to display advertisements on your computer, redirect your search requests to advertising websites, and collect marketing-type data about you – for example, the types of websites that you visit – so that customized adverts can be displayed.

Other than displaying advertisements and collecting data, adware doesn't generally make its presence known.

Sometimes there will be no signs of the program in your computer's system and no indication in your program menu that files have been installed on your machine.

There are two main ways in which Adware can get onto your computer:

Via freeware or shareware: Adware can be included within some freeware or shareware programs as a legitimate way of generating advertising revenues that help to fund the development and distribution of the freeware or shareware program.

Infected websites: A visit to an infected website can result in unauthorized installation of adware on your

machine. For instance, adware can access your computer via a browser vulnerability and then install trojans. Adware programs that work in this way are often called browser hijackers.

Creepy Ads

Many consumers feel uncomfortable being shown ads that include personalized elements, such as their name (like in the Coca Cola ad on Twitter which includes the person's name - Christopher).

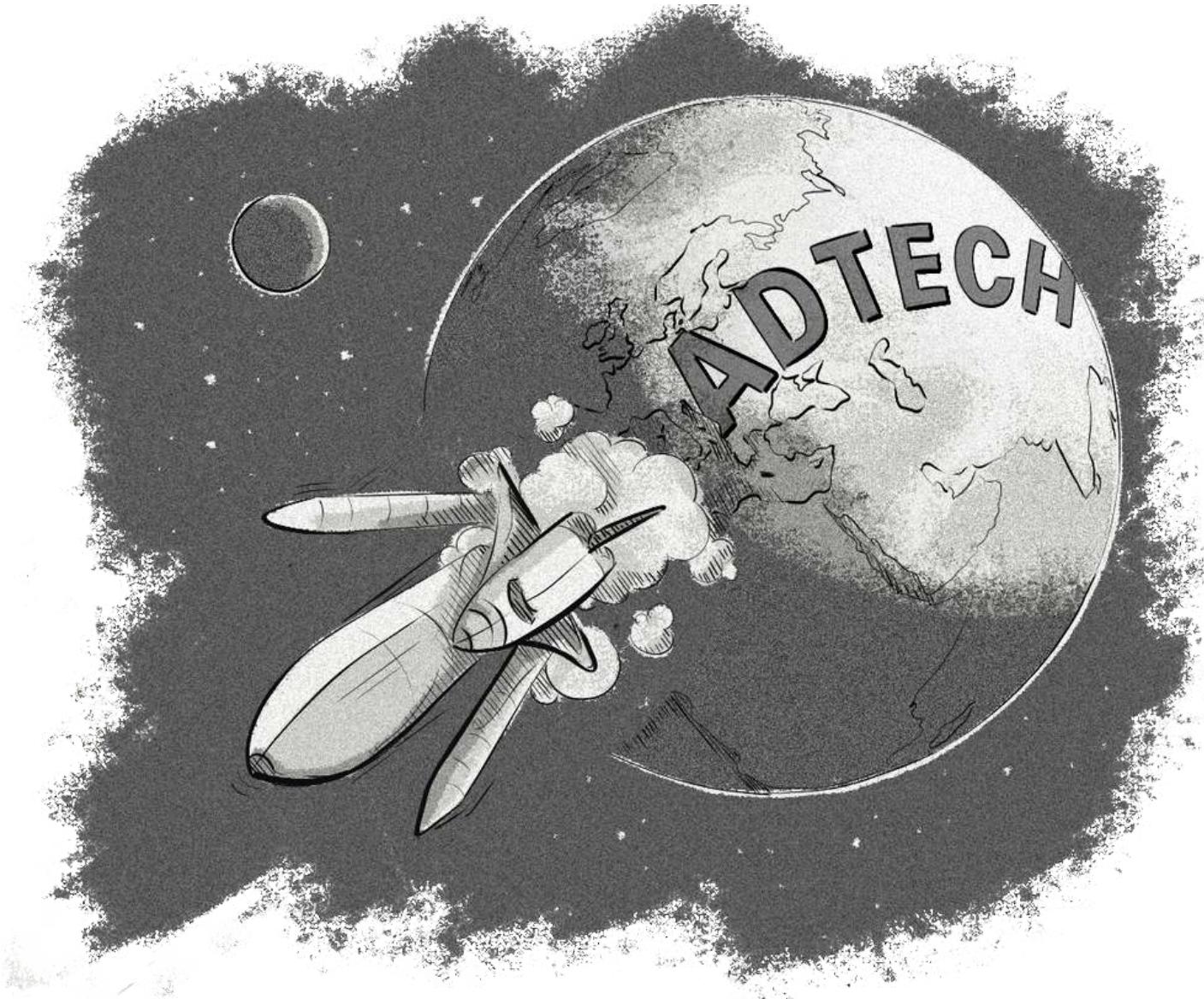
Also, many don't like being shown retargeted ads that display a product or service they looked at previously as they feel like they are being followed around the Internet and that ad companies know too much information about them.

The Future of User Privacy in Digital Advertising

With all the advancements in user privacy over the past few years, AdTech companies should be planning for the future by making changes to their tech to make it privacy friendly and compliant with privacy laws, and staying up to date with new announcements around the privacy settings in web browsers (e.g. ITP and Privacy Sandbox).

With all that's been happening in digital advertising over the past 5 years regarding privacy, it's clear that the future of digital advertising lies in privacy-friendly tech and processes.

15. AdTech From The Vendors' And Agencies' Perspective



So far in this book we've mainly been focusing on technical topics and the relationship between advertisers and publishers, but in this chapter, we'll briefly cover the business side of AdTech and what that looks like for technology vendors (e.g. DSPs and SSPs) and advertising agencies.

AdTech from the Vendor's Perspective

To summarize AdTech from the vendor's perspective, we'll look at two main areas: AdTech business models and the main technical challenges with running an AdTech company.

AdTech Business Models

The two most common business models employed by AdTech companies are **fixed CPM** and **a percentage of the media cost**, but many AdTech companies are switching to, or at least incorporating, the traditional usage model found at other software-as-a-service (SaaS) companies.

Here's an overview of the main pricing models used by AdTech vendors today:

Business model	Description
Fixed CPM	Clients pay a fixed cost per mille for every impression served.
Percentage of media spend	Clients pay a percentage of the media cost. So if an advertiser buys inventory at \$1.50 CPM, the DSP it uses to buy the inventory could charge 10%, meaning the total cost of the ad for the advertiser would be \$1.65.
SaaS	Clients pay a set price per month based on the number of users (aka seats). There are many variations of the SaaS pricing model and many vendors can incorporate elements of it and combine it with the fixed CPM and percentage of media spend models.

To read more about the above models, we recommend this article by [Beewax's](#) co-founder and CEO, Ari Paparo: [The Entrepreneur's Guide To Ad Tech Business Models](#)

The Main Technical Challenges of Running an AdTech Company

Although the technical challenges AdTech companies face vary from company to company, there are a few that all AdTech vendors would experience:

Performance and scalability: Due to the real-time and fast nature of programmatic media buying, AdTech vendors need to ensure their platforms can handle large volumes of bid requests per second and produce reports within a short period of time, e.g. showing analytics data within 15 minutes of the impression being displayed. This is critically important for platforms like DSPs and SSPs that have only 100ms to conduct an RTB auction.

Keeping infrastructure and cloud computing costs down: Because many AdTech platforms handle large volumes of traffic (e.g. ad requests and responses), it's important for them to keep infrastructure and cloud

computing costs down. One way to achieve this is to optimize their cloud computing architecture and select better performing systems (e.g. databases).

Finding developers with skills and experience in building AdTech platforms: Designing and building AdTech platforms is much different than building other types of software and there's a long and steep learning curve attached to it. Building AdTech platforms requires understanding of how the different players and platforms in the digital advertising ecosystem work and connect together. Finding developers or development companies with knowledge, experience, and skills in building AdTech platforms is a huge challenge for many companies.

AdTech from the Advertising Agencies's Perspective

As we mentioned earlier in [Chapter 04. The Main Technology Platforms and Intermediaries in the Digital Advertising Ecosystem](#), many brands have traditionally partnered with advertising agencies to help them with pretty much every aspect of their advertising campaigns, from creating the ads to running the campaigns across multiple publishers.

But thanks to advertising technology, some brands are taking some of the digital media-buying activities in-house.

In-House Programmatic Vs In-House AdTech

You'll often hear folks in digital advertising talk about in-house AdTech and in-house programmatic.

In-house programmatic: When a brand uses their own AdOps teams to run ad campaigns in external AdTech platforms.

In-house AdTech: When a brand or advertising agency builds their own advertising technology platforms, such as ad servers, DSPs, SSPs, and DMPs.

Below we'll look at the three main variations of the in-house model for brands and ad agencies.

1. The Traditional Way of Buying Digital Media

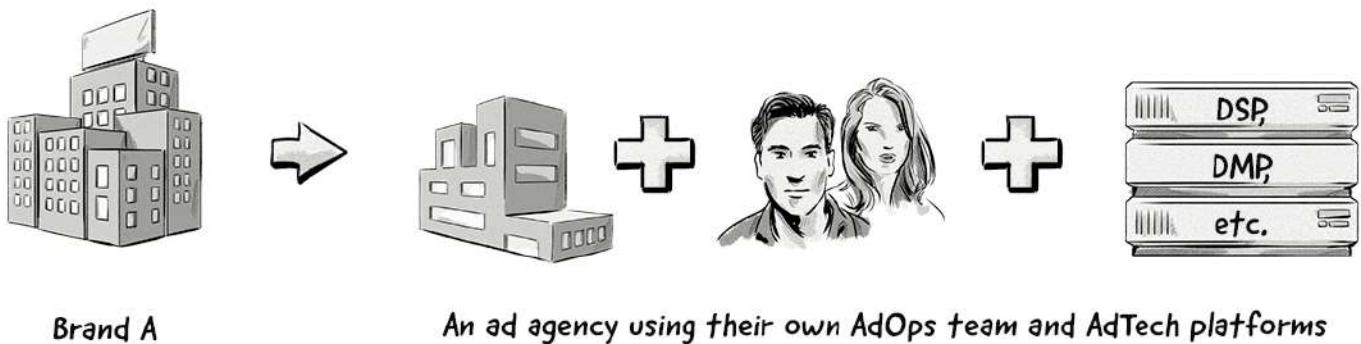
In this first example, a brand uses an advertising agency for their advertising campaigns. The advertising agency's AdOps team would then use external AdTech platforms to execute and manage the campaigns.

This is how most brands and agencies operate.



The main advantage of this arrangement is that the brand can outsource all of its advertising activities to the ad agency. The ad agency would handle all aspects of the advertising campaigns, including designing the creatives, setting up the campaign in AdTech platforms (e.g. ad servers and DSPs), launching the campaigns, and optimizing them to improve performance.

2. An Ad Agency Takes Programmatic Buying and AdTech In-House



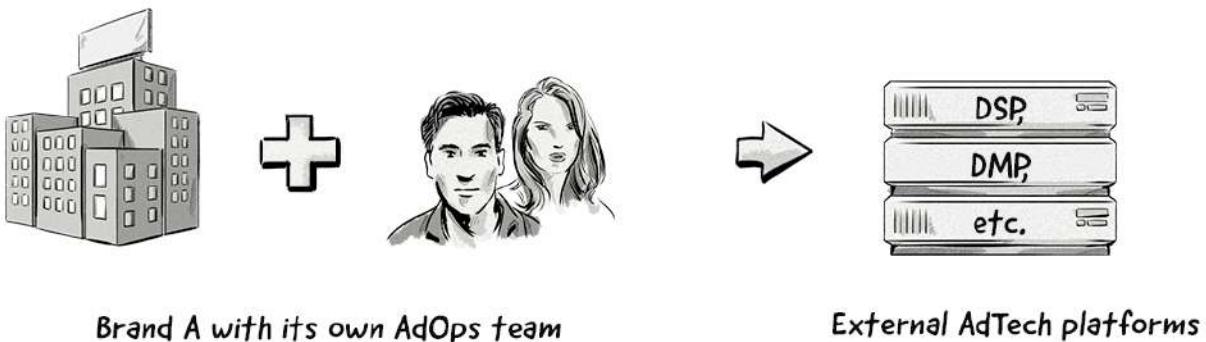
In this third example, an agency has its own in-house AdOps team and its own in-house AdTech platforms.

The biggest advantage of taking all aspects of programmatic buying and AdTech in-house is control and ownership of the technology and data, which will provide the agency with transparent insights into the true cost of its media spend and audiences.

The main disadvantages of this setup would be costs. Building AdTech platforms requires a big financial investment in the beginning and then an ongoing investment to maintain the AdTech platforms.

Therefore, this sort of situation is mainly reserved for large agencies whose revenues from media campaigns are enough to justify the large financial investments in building and maintaining AdTech platforms.

3. A Brand Takes Programmatic Buying In-House



In this example, a brand bypasses the ad agency and uses an in-house AdOps team and external AdTech platforms.

For brands, there are a number of advantages of taking programmatic media buying in-house. The main ones being cost savings as the brand doesn't have to pay an ad agency, and more control over their data, ad placements, and audience relationships.

However, bypassing an ad agency means that brands miss out on some of the most critical parts of any successful ad campaign like brand development, advanced marketing tactics and methods, and large amounts of creativity, which are all provided by ad agencies.

4. A Brand Takes Programmatic Buying and AdTech In-House

In this situation, a brand takes both programmatic media buying and AdTech in-house.

Just like in the example above, one major drawback is the absence of creativity and experience that's provided by ad agencies.



The main advantages of in-house programmatic and AdTech for brands are control, transparency, and cost savings.

By using their own AdOps team and AdTech platforms, brands will have much more control over their data and relationships with their supply-side partners and publishers, and have greater transparency into the

media-buying process (e.g. which partners are delivering the best results and the real cost of their bids).

Brands will also save money on fees and commissions, however, these cost savings will only appear after they've paid off the original investment in building the tech. Also, if a brand doesn't spend enough on media, then they might not have any long-term cost savings at all.

Advertising Technology: The Build vs Rent Dilemma

As we saw in examples 2 and 4 above, some ad agencies and brands have built their own AdTech platforms.

Below we take a look at the advantages and disadvantages of this topic from both the business and technology perspective.

Build vs Rent: From The Business Perspective

Build	Rent
<p>Advantages:</p> <ul style="list-style-type: none">• Reduce mark-up on media spent.• More transparency on the cost of the media.• Intellectual property ownership.• Can increase company value. <p>Disadvantages:</p> <ul style="list-style-type: none">• Relatively high upfront costs to build or acquire the technology.• Ongoing maintenance and operational costs.• Additional risks due to inexperienced staff.	<p>Advantages:</p> <ul style="list-style-type: none">• Access to industry experts.• A dedicated support team.• The ability to start running campaigns straight away.• Typically low or no upfront costs. <p>Disadvantages:</p> <ul style="list-style-type: none">• Fees and commissions.• A lack of transparency into the cost of media buys etc.

From The Technology Perspective

Build	Rent
<p>Advantages:</p> <ul style="list-style-type: none">• Control of the data.• Control of the platform's features and roadmap.• Custom proprietary features and algorithms. <p>Disadvantages:</p> <ul style="list-style-type: none">• Long learning curves for your in-house team.• Lengthy implementation and rollout processes.	<p>Advantages:</p> <ul style="list-style-type: none">• Instant access to a range of fully developed features.• Access to a vast range of inventory & data sources. <p>Disadvantages:</p> <ul style="list-style-type: none">• There's often a lack of or limited customization possibilities.

16. Programmatic & AdTech in 2022: Challenges and Opportunities



Throughout this book, we've explained how many different areas of programmatic advertising and AdTech work.

In this chapter, we'll list the main challenges and opportunities in the web, in-app mobile, CTV and OTT, and DOOH industries.

The Main Challenges and Opportunities in Web Advertising

Identity and Privacy

In programmatic advertising, identity refers to the process of identifying individual users across different websites, mobile apps, or other devices.

Identity powers many key AdTech processes, including:

- Behavioral targeting
- Retargeting
- Frequency capping
- Measurement
- Attribution
- Ad fraud detection

The Challenges

For the past decade, third-party cookies have been the main mechanism for identifying online visitors in web browsers, but this is changing fast.

Over the past few years, there's been a big movement towards strengthening online user privacy. And in digital advertising, strengthening user privacy typically means making it harder for companies to identify individuals across different websites, mobile apps, and devices.

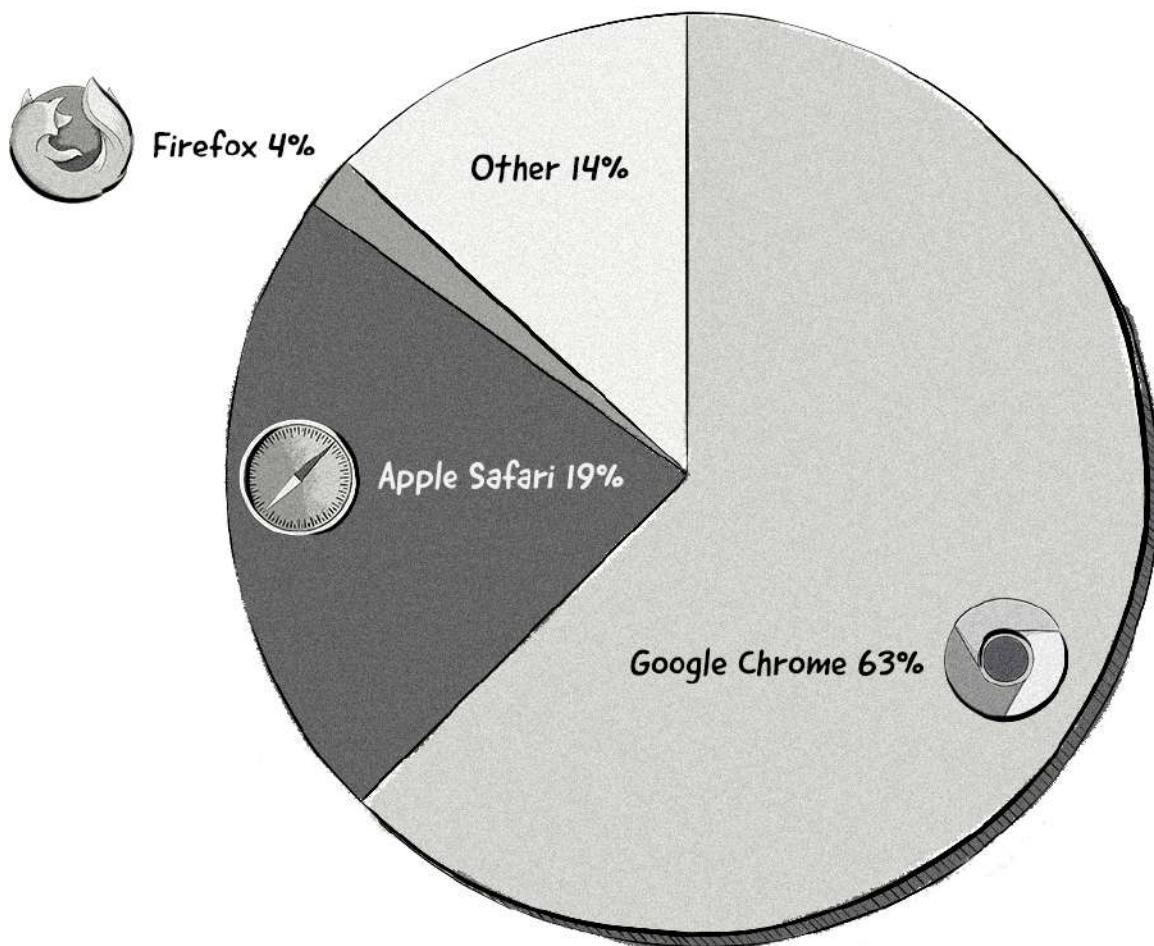
We've seen the introduction of privacy laws like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as well as many other privacy laws in other countries.

We've also seen many popular web browsers strengthen privacy for their users by limiting or blocking identification methods.

Safari and Firefox already block third-party cookies by default, and in January 2020, Google Chrome announced that it would be shutting off support for third-party cookies in Chrome by 2022. Chrome then announced in June 2021 that it won't be shutting off third-party cookies until 2023.

When Google Chrome finally does pull the pin on third-party cookies, it will have a much bigger impact on programmatic advertising than Safari and Firefox have had so far because of Chrome's global market share.

Web browser market share – global



Source: StatCounter, November 2019 to November 2020

The changes made by Safari and Firefox have given the programmatic advertising industry a preview of what a world without third-party cookies looks like, and it's not pretty.

For the most part, publishers have seen CPMs decrease and advertisers have noticed their addressable audiences shrink.

In 2022, all players in the programmatic advertising industry, from advertisers and agencies to tech vendors and publishers, will need to evaluate their identity strategies and look for solutions that solve their problems, which may differ from one company to another.

Opportunities

For most companies, the opportunities will come in the form of solutions already available on the market. For others, there are opportunities to innovate and build new tech to power the future of identity or meet their business goals.

Below is an overview of the solutions available to brands and agencies, tech vendors, and publishers:

Advertisers and agencies

In the past, advertisers and agencies have utilized third-party data to expand the size of their addressable audiences and reach more of their target audiences.

The privacy changes mentioned above have reduced the availability of third-party data, leaving advertisers and agencies looking for new ways to reach their audiences.

Here are just some ways advertisers and agencies can navigate the identity challenges in 2022:

First-party data: Most brands collect a treasure trove of first-party data, whether it's from their website, mobile apps, CRM platforms, ecommerce tools, or offline systems.

But simply collecting this data isn't enough. Advertisers and agencies will need to activate it, and one way they can do this is via an ID resolution service.

ID resolution services and ID graphs: Although some advertisers are moving away from behavioral targeting and towards other targeting methods, such as contextual, there are many that still see more value in being able to identify members of their audience across different websites and devices.

But with the availability of third-party cookies declining and mobile IDs facing a similar fate (at least, Apple's IDFA for now), advertisers will have to utilize a new set of tools to run identification, targeting, and attribution.

And ID resolution services and ID graphs are good options to explore.

ID resolution services and ID graphs aim to piece together IDs from online and offline channels to create a centralized view of consumers that can identify them across different websites, apps, and devices.

From there, advertisers can run behavioral targeting, retargeting, frequency capping, measurement, and attribution.

Contextual targeting: There's been a lot of talk in the programmatic industry about the revival of contextual targeting.

Even though some advertisers won't see the same campaign performance from contextual targeting as they do from other targeting methods like behavioral or retargeting, others may find that this type of targeting is more effective.

Because of its revived popularity, advertisers can expect to see more tools and options for contextual targeting in 2022 and beyond.

Tech vendors

For tech companies, the challenges around privacy have brought about platform consolidation, thrown up all kinds of obstacles, and threatened their business models.

But despite the challenges, tech companies actually stand to benefit the most from the current situation.

Advertisers will still need to advertise and publishers will still need to monetize their audiences. The changing privacy landscape isn't going to bring an end to digital advertising, it will just change the way it's done.

Also, the solution to many of these challenges is a technological one.

Below are just some opportunities that tech vendors can take advantage of:

Build identity resolution services: Although there are already a number of ID resolution services and ID graphs on the market, there are some AdTech and MarTech vendors that could benefit from building their own ID tools and solutions and incorporating them into their current product offerings.

Build or update existing tech: The changing programmatic industry requires tech companies to change their tech. Whether it's incorporating new targeting methods (e.g. contextual), integrating with other platforms and tools, or building new tech, the successful AdTech and MarTech companies of the future focus on innovation and solve the various challenges with new technologies.

Innovation has also been a core component of programmatic advertising. We saw this with things like real-time bidding (RTB) and we'll see it again with the challenges around identity and privacy.

Publishers

The challenges and opportunities that publishers face regarding identity and privacy are very similar to those that advertisers face.

For publishers, the fact that third-party cookies are no longer available in Safari and Firefox and will soon be scrapped from Chrome means that they're not able to identify their audience on the same scale as they used to, resulting in advertisers paying lower CPMs because they're not able to identify their target audiences.

This has caused publishers to look for solutions that will enable them to continue identifying their audiences, or at least part of their audience, and bolster their monetization strategies.

First-party data: Out of all of the players in the programmatic advertising industry, publishers are the only ones that have direct access to the most prized asset of all; audiences.

Sure, some advertisers also function as publishers and have access to audiences, but publishers are the ones that hold the key to the castle.

The ever-growing challenges around privacy and identity have led publishers to focus on creating stronger relationships with their audiences and unlocking the potential of their first-party data.

Luckily for publishers, many AdTech and MarTech companies have also turned their focus to helping publishers unlock the value of their first-party data.

Examples include:

- The Trade Desk's [Unified ID 2.0](#).
- Independent identity providers like [ID5](#).
- ID resolution services and ID graphs like [LiveRamp](#), [Tapad](#), [Signal](#), [Zeotap](#), and [InfoSum](#).

Tech development investments: Traditionally, many publishers haven't seen the need to invest in tech development, but the privacy and identity challenges are providing publishers with the opportunity to not only solve these challenges via tech development, but also give them more control over their audiences and data.

In 2021, we saw many large publishers invest in tech development, and in 2022, we'll likely see an increase in publishers entering this space.

The New York Times, for example, has [built its own audience segments](#) that it offers to advertisers. By building out these audience segments based on its rich first-party data, it has taken ownership of its audience and provided a solution to a problem that is usually handled by tech companies.

While building new tech and tools, or even a small amount of custom tech development, won't suit every publisher, there are certainly many publishers that stand to benefit by making technology development a part of their monetization and growth strategy for 2022.

Google Chrome's Privacy Sandbox

There's also another solution that publishers, advertisers, ad agencies, and AdTech companies can explore; Google Chrome's Privacy Sandbox.

Chrome's Privacy Sandbox is a series of standards and APIs designed to replace the processes currently underpinned by third-party cookies.

The goal of Privacy Sandbox is to maintain targeted advertising and measurement for both advertisers and publishers, but do it in a much more privacy-friendly way.

Privacy Sandbox is currently being worked on in a W3C business group between Google Chrome, Google's ad product teams, and independent AdTech companies, publishers, advertisers, and agencies. Although some of the standards have been tested, it's not yet known when Privacy Sandbox will go live.

The Main Challenges and Opportunities in In-App Mobile Advertising

The mobile advertising industry has been on a constant incline over the past 5-10 years, but in 2022, the industry will face challenges it hasn't faced before.

Challenges

Apple's Privacy Changes

Traditionally, Apple's privacy crusade has been isolated to its Safari web browser, but in June 2020 at the Worldwide Developers Conference (WWDC), the tech giant announced a series of privacy changes to its upcoming release of iOS 14 that will have a negative impact on in-app mobile advertising.

Here's an overview of the privacy changes in iOS 14:

Apple's Identifier for Advertisers (IDFA)

Apple announced that it will be releasing a new feature in its mobile devices known as the App Tracking Transparency (ATT) framework.

This feature will require app developers to obtain permission from users before collecting the device's identifier for advertisers (IDFA) and passing it to AdTech companies, such as ad networks, supply-side platforms (SSPs), and mobile measurement platforms (MMPs).

Apple's IDFA is a string of random numbers and letters assigned to Apple devices like iPhones, iPad, and Apple TVs.

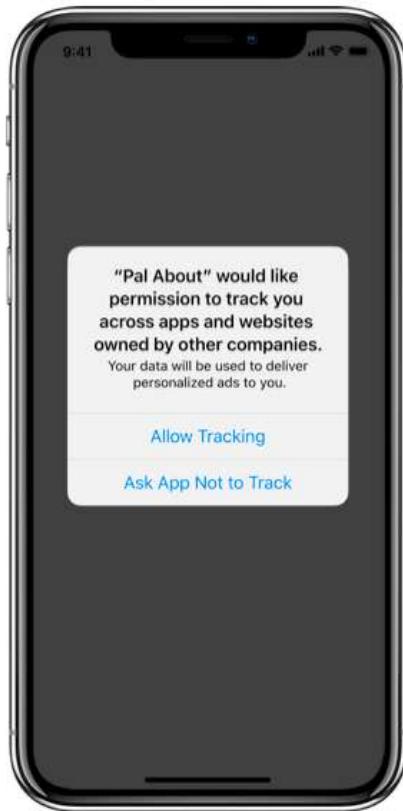
Advertisers can use the IDFA to identify iOS, iPadOS, and tvOS users across different apps to deliver personalized and targeted advertising, run frequency capping, measure campaign performance, and attribute impressions and clicks to app installs.

Here's an example of what an IDFA could look like:

7D902I08D-7846-4CA4-TE6P-83369125YFDC

A device's IDFA can be accessed by the app's developer and then passed on to different AdTech platforms. However, Apple's changes to its IDFA means that before a device's IDFA can be accessed by a mobile app developer, they'll first need to get consent from the user using the ATT framework.

Users will be shown a message similar to the one below and asked to make a choice:



If the user selects the *Allow Tracking* options, then the IDFA will be passed as usual. If the user doesn't allow the app developer to access their IDFA, i.e. selects *Ask App Not to Track*, then the IDFA will be zeroed out, making it useless from an identification point of view.

The mobile app developer will only be able to ask the user for access to their IDFA once per install. Nobody knows for sure but most estimates put the opt-in rate between 1% to 20%.

Tim Koschella, CEO at Kayzan, [posted some figures](#) that show the initial opt-in rates were around 15% to 20%. However, it's still early days and the opt-in rates will depend on a number of factors, such as the vertical (gaming vs dating) and whether app developers have displayed their own message to users before showing them the ATT message.

As you can imagine, it's likely that most users will select the Ask App Not to Track option, meaning the IDFA won't be as readily available as it is now. This will have a negative impact on the performance of in-app mobile advertising campaigns as ad targeting and attribution will be less accurate.

We've already seen companies like Facebook, Snapchat and Twitter [reportedly post losses totalling \\$10 billion USD](#) as a result of Apple's IDFA changes. Many other companies operating in the in-app advertising industry would have also seen their revenues fall. We'll likely see similar stories emerge in 2022.

Apple's SKAdNetwork

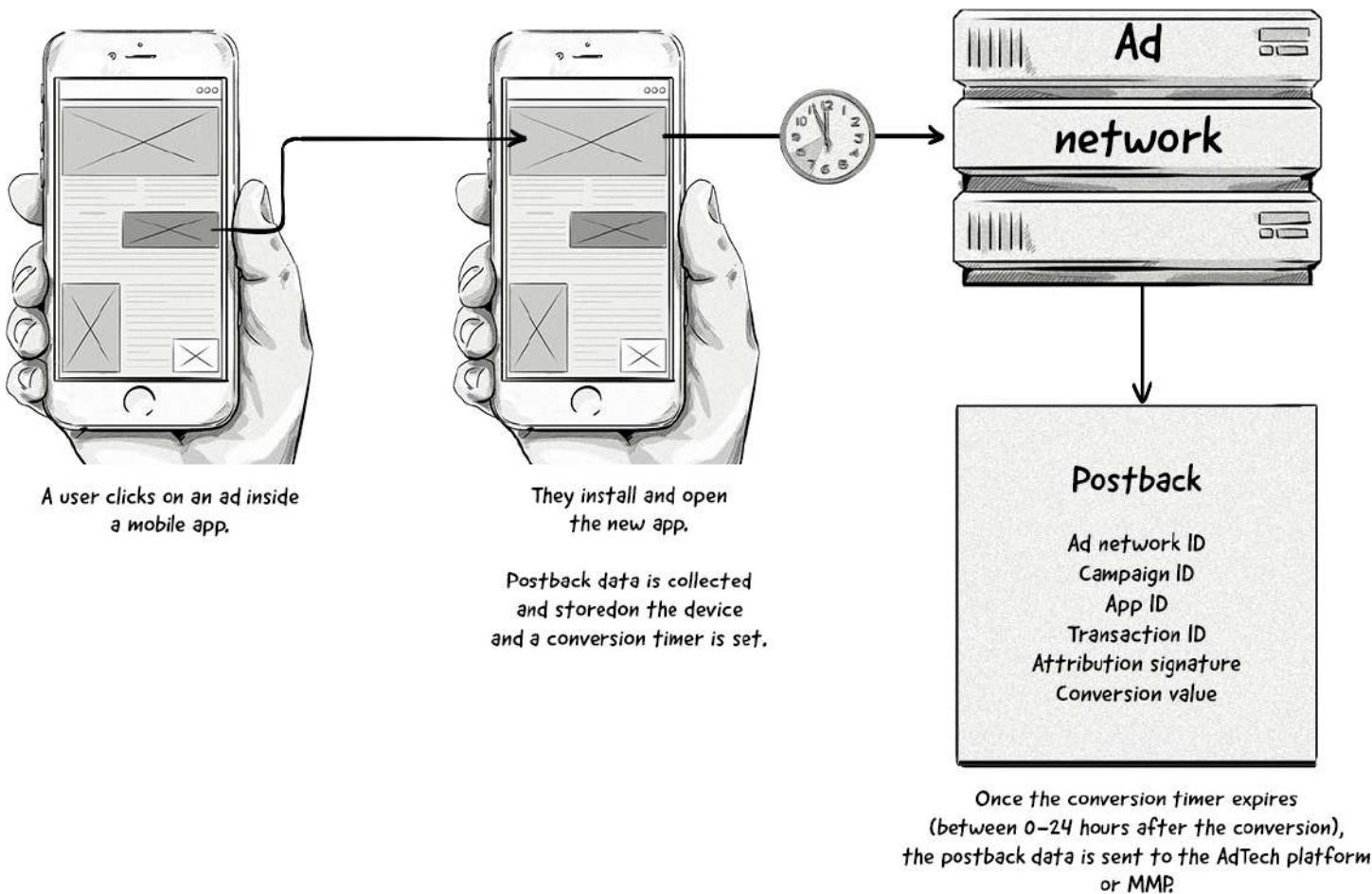
Although Apple hasn't offered up any kind of solution for ad targeting, it has proposed a tool for attributing ad clicks to add installs. And it's called SKAdNetwork.

Apple's SKAdNetwork is designed to provide advertisers with conversion data without revealing any user-level or device-level data. It's Apple's version of a privacy-friendly way to attribute app installs.

Here's how Apple's SKAdNetwork will work:

How Apple's SKAdNetwork API works

The SKAdNetwork is designed to attribute ad clicks with app installs in a privacy-friendly way.
No user-level or device-level data is passed to AdTech platforms or MMPs.



A couple of points about the SKAdNetwork:

- The IDFA won't be passed to AdTech platforms or MMPs, even if the user has opted in.
- All attribution data will pass through SKAdNetwork and then onto the AdTech platform or MMP.
- SKAdNetwork will only attribute app installs (via the last-click model) and not view-through conversions.
- Campaign IDs are limited to 100 per AdTech platform (e.g. ad network or MMP).

Privacy Report and ITP for All Browsers in iOS 14, iPad 14, and Safari 14

In addition to the AppTrackingTransparency framework, Apple also announced a couple other [privacy changes in iOS 14](#):

1. Privacy Report: Users will now be able to see how many trackers were blocked by Safari on a given page, as well as other information about trackers.
2. ITP for all web browsers: For iOS 14 users, ITP will be applied to all web browsers, not only Safari.

This means that all web browsers, not just Safari, in iOS (v14 and above) will include the Intelligent Tracking Prevention feature.

WWGD = What Will Google Do?

Ever since Apple announced its changes to its IDFA, many people in the industry asked the question, “Will Google make changes to its mobile ID?”

In May 2021, Google announced that it will require [app developers to include privacy information](#) in their Google Play Store listings, similar to the privacy information displayed in Apple’s App Store listings.

Then in July 2021, Google announced that it would [stop passing on its AAID](#) if the user had opted out of personalized advertising. These changes went live with the release of Android 12 in the later part of 2021. While this is considered a privacy change, it’s not as stringent as the ones released by Apple.

Opportunities

Just like with the privacy challenges in web browsers, the main opportunity here for companies is to create solutions that will allow advertisers to reach their target audience and measure the performance of their ad campaigns, and help mobile app developers to continue their app monetization strategies via advertising.

But this won’t be easy, and in some ways it will be harder to solve the IDFA challenges than it will be to solve the third-party cookies challenges in web browsers.

The Main Challenges and Opportunities in CTV and OTT

The hype around the connected TV (CTV) and over-the-top (OTT) industries is akin to the hype around mobile in the late 2000s.

There’s a lot happening in the CTV and OTT worlds, and just like all new channels, they are experiencing a few teething problems.

Challenges

The main challenges in the CTV and OTT advertising industries are:

Fragmentation

Unlike the fragmentation of tech platforms and devices that we’re used to seeing, the fragmentation issue in CTV and OTT runs much deeper.

Firstly, every CTV device has its own hardware and software, meaning they all have their own IDs (some don’t have any!). This makes it difficult to create any kind of unified identifier across all of the different CTV devices.

Also, the fact that a consumer might use multiple devices to watch video content across different OTT services only exacerbates the problem. What this means for advertisers is that it’s quite hard to reach their target audience at scale within the CTV and OTT environments.

Identity

As mentioned above, the fragmentation of devices and apps is causing a lot of issues around identity.

Compare this to advertising in web browsers. If an advertiser wanted to reach their target audience, then the only real challenge would be identifying them across different browsers (ignoring for a moment the various privacy challenges around identity in web browsers).

Even though there are many web browsers available, most people use Google Chrome and don't tend to switch between web browsers.

In the CTV and OTT environments, there are multiple CTV devices and multiple OTT apps, meaning identifying audiences across all of those devices and apps is a huge challenge.

To help alleviate these identity challenges, the [IAB Tech Lab has released a set of guidelines](#) to help companies operating in the CTV and OTT industry use and pass the correct ID from the various devices to OTT apps and AdTech platforms.

Measurement

The key to accurate measurement and attribution in digital advertising is identity. And as you saw above, there are many challenges around identity. In the short term, this means measuring the performance of CTV and OTT campaigns and attributing ad views to conversions will be limited at best.

When it comes to viewability and measurement, there are a few key challenges that need to be addressed:

- **Identifiers:** The lack of a consistent identifier across all the different CTV devices means that identification is fragmented and limited.
- **Access to devices:** Most CTV devices are closed off, meaning third-party verification tools have restricted access.
- **Server-side ad insertion:** Server-side ad insertion is a common way to serve ads inside CTV and OTT environments, but it presents many challenges (listed in the next section). Because of the way SSAI is set up, it is harder to identify invalid traffic (IVT) and collect measurement data.

To help address these key challenges, the IAB has been working on refining some of its existing standards, specifically, VAST and OM.

The video ad serving template (VAST) is an IAB standard that is used in video advertising in both web browser and in-app mobile environments. Although VAST is responsible for video ad serving, it doesn't handle the measurement side of video advertising. For that, there's video [Video Player Ad Interface Definition \(VPAID\)](#).

However, VPAID will soon be deprecated and the measurement function of VPAID will be replaced with the open measurement (OM) standard.

The goal of OM is to not only power measurement for video advertising in web browser and in-app mobile environments, but also in CTV and OTT environments.

The IAB is continually working on both VAST and OM to help standardize the ad serving and measurement processes within the CTV and OTT environments.

Ad Serving

Server-side ad insertion is becoming the main way to serve ads in CTV and OTT environments. Although SSAI is an improvement on CSAI, it does have a couple of drawbacks.

For starters, it's vulnerable to ad fraud as it's not easy to identify if the ad requests are coming from an actual AdTech platform or whether there's a fraudster on the other end. Because of this, it is also hard for invalid traffic detection tools to tell the difference between genuine and fake traffic.

Secondly, it's harder to incorporate IAB standards, such as VPAID and older VAST versions, into SSAI.

But as mentioned above, the IAB Tech Lab is working on updating the existing video ad-serving standards VAST and OM to support ad serving and measurement.

Ad Fraud

Ad fraud has been a constant challenge in programmatic advertising for the best part of a decade, with fraudsters following the money; from display to mobile, and now, to CTV and OTT.

Just like with other channels, fraudsters have been looking for the vulnerabilities and opacity to carry out and conceal their fraudulent activities.

Some of the main CTV and OTT ad fraud schemes that have been detected so far include [ParrotTerra](#), [StreamScam](#), LeoTerra, Colorius, [ICEBUCKET](#), [DiCaprio](#), and [Monarch](#).

The fact that the CTV and OTT industry is still fairly new, it's not really surprising that we've seen so many ad fraud schemes already.

As the industry matures, we'll likely see more [IAB standards like app-ads.txt](#) be adopted, which will help address and hopefully eradicate some of the ad fraud schemes listed above.

But as we've seen in other digital advertising channels, ad fraud is a constant theme that is difficult to eliminate completely.

Opportunities

The main opportunity here is to address and solve these challenges via technical innovation.

Out-Of-Home (DOOH)

Challenges

The main challenge facing the out-of-home (DOOH) industry is returning to the pre-pandemic levels of both ad spend and investment in technology.

Prior to the COVID19 outbreak, the OOH industry was one the fastest growing digital advertising industries, with most of this growth originating from digital out-of-home (DOOH).

When most cities around the world went into lockdown, the OOH market was one of the hardest hit.

According to research from eMarketer conducted before March 2020, ad spend on OOH in the US was set to grow by 3.3% in 2020, with ad spend totalling US\$8.87 billion. Adjusted forecasts in June 2020 put the total ad spend for 2020 at US\$8.25 billion.

In the UK, a report by the Advertising Association and Warc showed that ad spend on [OOH fell by 70.4% in the second quarter of 2020](#).

Apart from the impact of the pandemic, other challenges in the DOOH industry revolve around inventory availability, audience targeting, and measurement and attribution.

Opportunities

The opportunities in DOOH lie in solving the many technical challenges the industry faces.

The addition of the digital, and programmatic, element of out-of-home means that companies need to invest in developing the technology that will allow DOOH to mirror the other digital forms of advertising, such as display and in-app mobile.

But this is challenging, mainly because it's much harder to set up a DOOH ad campaign than it is to set up a traditional display ad campaign. However, as more investment goes into DOOH, the gap between what's possible currently with DOOH and what isn't will decrease.

Another Topic to Keep an Eye on in 2022

The topic below isn't a challenge, but rather an industry trend that we'll likely see more of throughout 2022.

Antitrust investigations and Lawsuits Against GAFA

Over the past year or so, we've seen a number of governments around the world take aim at the dominance of Google, Amazon, Facebook, and Apple in the form of antitrust investigations.

This is an area worth keeping an eye on as it may lead to some of the walled gardens spinning off some of their products and companies, which may impact independent AdTech companies and the programmatic advertising industry (likely, in a positive way).

Below are the main antitrust investigations that have began so far:

The UK's Competition and Markets Authority Investigates Google Chrome's Privacy Sandbox

On January 8, 2021, the UK's competition watchdog opened an investigation into Google's intent to eliminate third-party cookies and other functions from Chrome browser that would negatively affect the advertising and marketing industry.

Online Publishers Sue Google in Advertising Antitrust Lawsuit

On Wednesday October 20, 2020, Genius Media Group together with The Nation put forward a lawsuit seeking justice over Google, claiming that it has hurt their businesses by controlling advertising opponents and displaying anticompetitive conduct.

The US Department of Justice (DOJ) Investigates Google

On Tuesday October 20, 2020, the US Department of Justice (DOJ) opened an investigation into Google's dominance of its search and search advertising businesses.

A Bipartisan Group of State Attorneys General Sue Google

In December 2020, a bipartisan group of state attorneys general from 38 states sued Google for anticompetitive conduct relating to its search and search advertising businesses.

The lawsuit is very similar to the DOJ's lawsuit (listed above) but provides more examples of Google's anticompetitive behavior to secure the dominance of its services (e.g. search engine and mobile apps).

Republican Attorneys from 10 States Sue Google Over Anticompetitive Behavior in the Digital Advertising Market

On Wednesday December 16, 2020, the Republican attorneys from 10 states sued Google for its dominance of the digital advertising market.

The main allegations are that Google overcharged advertisers, boxed out competitors and squeezed publishers, adding up a monopoly tax on businesses.

The FTC and Attorneys General Sue Facebook Over Illegal Monopolization of the Social Networking Market

On Wednesday December 9, 2020, the US Federal Trade Commission (FTC) and 48 attorneys general sued Facebook for alleged illegal monopolization of the social networking market.

Although both of these lawsuits are separate, they were both announced at the same time and concern the same topic; Facebook's violation of antitrust laws.

The Australian Government Introduces a New Media Bargaining Code to Make Google and Facebook Pay for Distributing News

While most governments are opening antitrust investigations into Google and Facebook, the Australian government has decided to tackle the duopoly's dominance in a different way.

In December 2017, the Australian Government asked the Australian Competition and Consumer Commission (ACCC) to open an inquiry into Google and Facebook to determine the impact those companies have on competition in the media and advertising markets in Australia.

Then in July 2019, the ACCC released the final report and executive summary. For the most part, the code would require Google and Facebook to negotiate deals with media companies whereby the tech giants would pay them for the content they distribute.

After some initial backlash, which included Google threatening to block Australians from Google Search and Facebook temporarily blocking accounts of news sites, both Google and Facebook have agreed to make deals with Australian news companies.

THE END



CLEARCODE

Questions, queries or comments?

If you have any questions about the contents of this book, happen to find any errors, or simply want to provide feedback, then please contact us via adtechbook@clearcode.cc

We can also be contacted via the following channels:

Web: clearcode.cc

LinkedIn: linkedin.com/clearcode

Twitter: [@clearcodehq](https://twitter.com/clearcodehq)

Facebook: facebook.com/clearcode