Google

Navigate the new ads landscape

2022

A playbook of privacy-forward solutions from Google

Overview

At a glance

Growing user concerns about privacy have set in motion a series of changes that will reshape the digital advertising ecosystem for years to come. With rising user privacy expectations, new global regulations, and browser and operating system changes, the shift to a privacy-first future is quickly approaching.

Google values the success of publishers and their vital role in the ad-supported open Internet. We support publishers of all sizes as they navigate today's privacy environment.

This playbook outlines the Google solutions and strategies available to publishers.

This playbook features interactive elements to help you quickly navigate to the content that matters most to you. Use the ☰ Table of Contents to jump ahead to the sections that interest you.

Throughout the playbook you'll find a **navigation bar** in the top left corner that will help you jump to various sections.

🔗 **Additional resources** will be linked in each section to help you take action.

Table of Contents

Section I

Preparing for a Privacy-forward Future

Overview

Given how quickly the privacy landscape is evolving, managing a digital advertising business can seem more complicated than ever. Thankfully, there are several ways for publishers to adapt to privacy trends to uncover new opportunities.

By testing new strategies and evolving their business practices, publishers can sustain and grow their revenues while respecting customer privacy preferences.

→ 01. Why Privacy Matters

→ 02. What’s at Stake for Publishers

→ 03. Google’s Approach & Vision

Jump to Section II to learn how regulations might impact your business →

Why Privacy Matters

Shifting Consumer Mindsets

Privacy is top of mind for many users, driven by a rise in consumer awareness and shift in data privacy expectations. (Source: EY Global Consumer Privacy Survey)

New research from a study conducted by Boston Consulting Group and Google shows that while two-thirds of consumers want ads that are customized to their interests, nearly half are uncomfortable sharing personal information in exchange for tailored ads.

Regulatory Response on the Rise

Global policymakers are introducing regulations to enforce responsible data practices that aim to meet consumer privacy expectations.

Regulatory scrutiny over how businesses collect and use consumer data is increasing worldwide. The shifting landscape is moving toward phasing out cross-web and device identifiers used for marketing and measurement.

What's at Stake for Publishers

In a recent Deloitte research study of publishers across the Americas, 90% of participants surveyed believe that online privacy changes are either overdue or arriving just on time.

$10B

As the industry shifts away from third-party cookies to honor an increasing preference toward privacy, a McKinsey report projected a $10B reduction in publishers' collective ad revenues in the U.S. alone.

In APAC, >60% of companies surveyed in the recent BCG Privacy Imperative research confirmed that privacy is important to people in their country, with >70% of them agreeing that not being privacy-ready will have significant consequences.

The report mentions that the drop in revenue will most likely have a disproportionate impact on smaller publishers who depend on data-driven ads for more than 80% of their ad revenue.

For publishers, lost revenue will mean less money to create new content, run their businesses, and pay their employees.

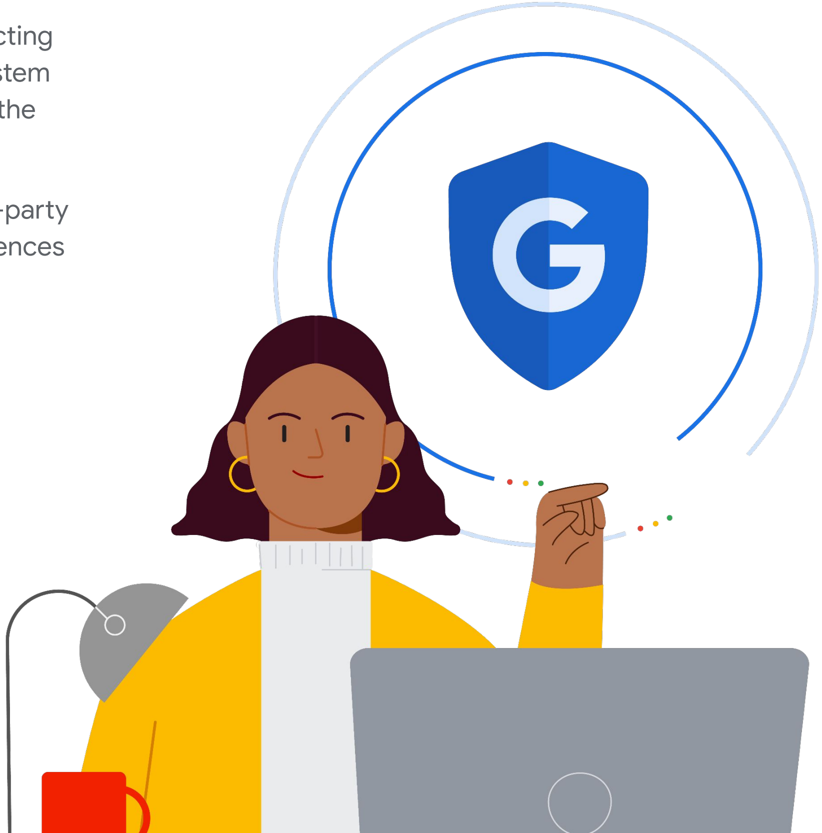
Building trust with customers is also a huge opportunity. As trust in your brand grows, so too does the information you can use to help make your marketing strategy more relevant and effective.

Understandably, there is a lot at stake. That's why it's critical for publishers to take proactive steps in preparing their businesses for the new advertising landscape. Google is investing substantially in a broad suite of solutions to help publishers sustain revenues in the privacy-centric future.

Google's Approach & Vision

Google supports the ad-supported open Internet while also protecting user privacy. We remain committed to preserving a thriving ecosystem where people everywhere can access ad-supported content with the confidence that their privacy choices are respected.

We believe publishers with direct relationships with users and first-party data should be empowered to customize and improve user experiences with more helpful advertising.



Google's Approach & Vision

Principles we believe to be true

1

First, we believe that user privacy and personalized advertising are not mutually exclusive.

We can have a thriving Internet where publishers create content, and people around the world can continue to access this ad-supported content while feeling confident that their data is protected.

2

Second, publishers with direct relationships with users, and first-party data, should be empowered to customize and improve user experiences with more helpful advertising.

3

Lastly, tracking individual users across the web and on apps is not privacy preserving.

We don't believe these types of solutions meet the spirit of the change users are asking for.

Section II

Managing Regulations & Consent

Overview

Google is committed to launching tools to support our partners with their compliance efforts. Read on to learn more about the available solutions designed to help navigate an increasingly complex regulatory ads environment.

- 01. Regulatory Landscape
- 02. Privacy & Messaging Tab
- 03. Supporting Publishers

Please note

Google tools do not guarantee regulatory compliance. Please consult with your legal counsel to determine if a given regulation applies to your business, and if so, which of our tools, if any, might assist with compliance.

Google is working to help our partners comply globally as it relates to our products

Key recent examples:

AADC (Age Appropriate Design Code)

Google offers multiple solutions to assist with safeguarding minors, **including TFUA (Tag For Under the Age of Consent)**

CCPA (California Consumer Privacy Act)

Introduced **Restricted Data Processing (RDP)**

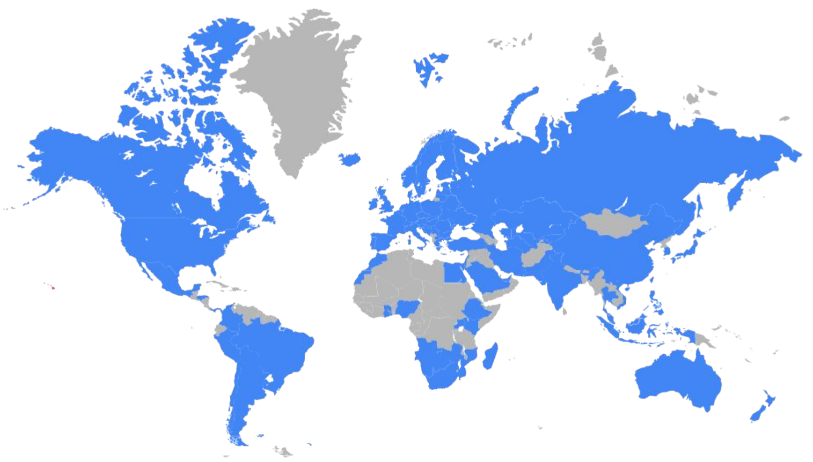
PIPL (Personal Information Protection Law)

For those publishers who determine they will require user consent for personalized ads, we offer **Non-personalized ads**

Beyond the recent examples above, Google has long provided publishers with tools to help them comply with GDPR.

Regulations are raising the privacy bar across the globe

The ads industry continues to see a rapid growth in regulation worldwide. We have several recommendations on how publishers can take action to better prepare for upcoming changes:



1. **Work with your legal team**
to ensure your privacy practices meet the requirements of the current laws, and work to better understand how future regulations may impact your business internationally.

2. **Be transparent about data collection and usage**
and make sure your privacy policy is up-to-date. Make it easy for people to understand what information is collected, how it's going to be used, who it may be shared with and why, and what value they'll receive should they give you permission to use their information.

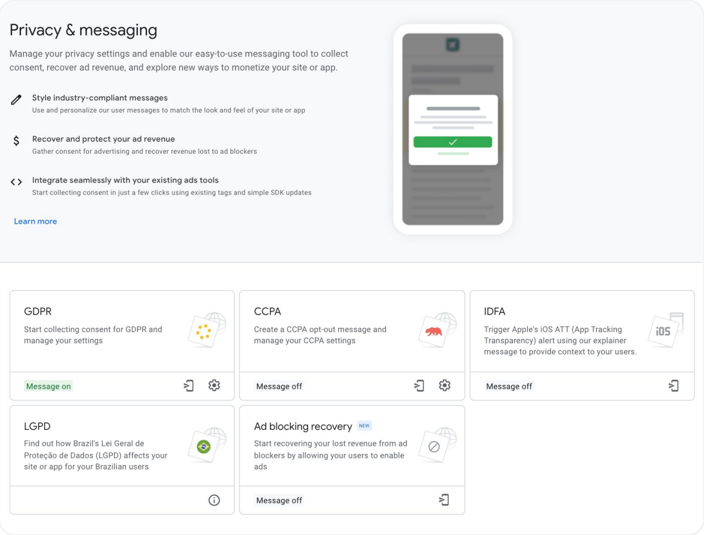
3. **Implement a Consent Management Platform (CMP)**
where appropriate to ensure your users have transparency into and control over how their data is used. While publishers with specific needs have the option to build their own consent solutions, using a CMP often makes it easier for publishers and developers to gather and manage consent from their website and app visitors. This way, they can deliver personalized ads, provide a better user experience, and continue to monetize their digital content.

Intro to Privacy & Messaging Tab

To help you better understand how different privacy regulations may impact your business, the Privacy & messaging tab offers you a single place to stay informed about relevant regulations, actions you can take, and optionally, to message your users and navigate the advertising landscape to mitigate impact to your business. Simply click on a card for information on:

- How the regulation may affect you
- How you can give users control
- Additional Google resources, such as website and developer documentation

Currently, the Privacy & messaging offers optional consent and opt-out messaging for GDPR and CCPA (web-only) respectively.



Privacy & messaging

Manage your privacy settings and enable our easy-to-use messaging tool to collect consent, recover ad revenue, and explore new ways to monetize your site or app.

Style industry-compliant messages
Use and personalize our user messages to match the look and feel of your site or app

Recover and protect your ad revenue
Gather consent for advertising and recover revenue lost to ad blockers

Integrate seamlessly with your existing ads tools
Start collecting consent in just a few clicks using existing tags and simple SDK updates

Learn more

GDPR
Start collecting consent for GDPR and manage your settings
Message on

CCPA
Create a CCPA opt-out message and manage your CCPA settings
Message off

IDFA
Trigger Apple's iOS ATT (App Tracking Transparency) alert using our explainer message to provide context to your users.
Message off

LGPD
Find out how Brazil's Lei Geral de Proteção de Dados (LGPD) affects your site or app for your Brazilian users

Ad blocking recovery NEW
Start recovering your lost revenue from ad blockers by allowing your users to enable ads
Message off

Google Product: Ad Manager | Ad Manager 360 | AdMob | AdSense

Platform: App | Web

Demand Type: Indirect | Direct

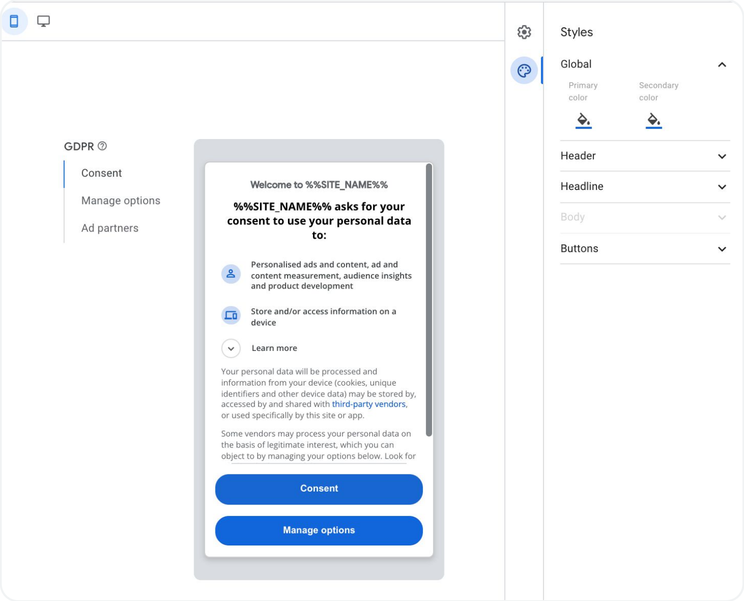
Please note *Google tools do not guarantee regulatory compliance*

Privacy & Messaging | Setting up GDPR Messages

Using the optional messaging features in Privacy & messaging, you can create and display a message to your users to help gather the consent required under the General Data Protection Regulation (GDPR). The message you create with Privacy & messaging lists the ad technology providers your site or app uses, and asks users to consent to the use of data for personalized ads and other purposes. You can also request consent for the use of data by your own site or app.

The GDPR message contains multiple “screens” (or “pages”) that are shown to users depending on which buttons and links they click in your messages. The button options presented to users are based on your selections in the “User consent options” section during message creation.

More information about configuring and deploying GDPR messages can be found in the following Help Center articles Ad Manager, AdSense, AdMob.



Welcome to %%SITE_NAME%%

%%SITE_NAME%% asks for your consent to use your personal data to:

Personalised ads and content, ad and content measurement, audience insights and product development

Store and/or access information on a device

Learn more

Your personal data will be processed and information from your device (cookies, unique identifiers and other device data) may be stored by, accessed by and shared with third-party vendors, or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for

Google Product Ad Manager | Ad Manager 360 | AdMob | AdSense

Platform App | Web

Demand Type Indirect | Direct

Please note *Google tools do not guarantee regulatory compliance*

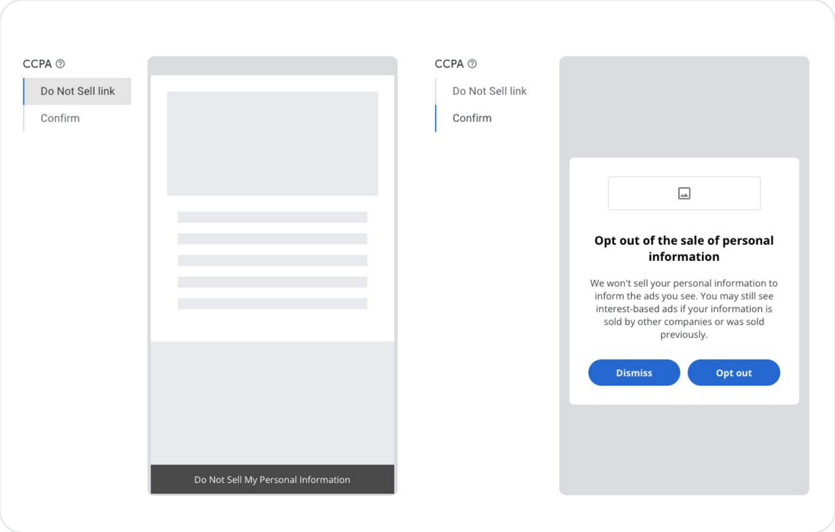
Privacy & Messaging | Setting up CCPA Messages

As part of CCPA, publishers must post a "Notice of Right to Opt-Out of Sale of Personal Information" (§ 999.306). The CCPA message type is displayed to users located in the US state of California and gives them the opportunity to opt out.

A CCPA message contains multiple "screens" (or "pages") that are shown to users when they view your message.

CCPA messages include the following elements:

- **Do Not Sell link:** The link to your CCPA message. Displays your "Do Not Sell My Personal Information" link using the formatting and settings you selected. When users click the link, the Confirm page opens and displays the "Opt out of the sale of personal information" dialog.
- **Confirm page:** The confirmation page of your CCPA message. Displays the "Opt out of the sale of personal information" dialog. Users can click the buttons to confirm their decision.



Opt out of the sale of personal information

We won't sell your personal information to inform the ads you see. You may still see interest-based ads if your information is sold by other companies or was sold previously.

Google Product Ad Manager | Ad Manager 360 | AdSense

Platform Web

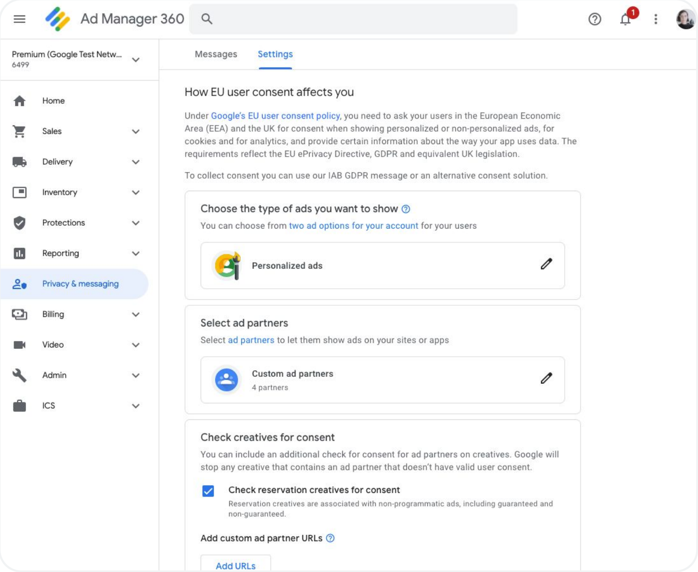
Demand Type Indirect | Direct

Please note *Google tools do not guarantee regulatory compliance*

Monetization in the Context of User Choice

In order to help support publisher compliance with GDPR, CCPA, and other relevant regulations, Google offers multiple solutions to assist with ads depersonalization. These solutions include Non-personalized ads, Limited ads, and Restricted data processing.

- **Non-personalized ads:** Non-personalized ads are ads that are not based on a user's past behavior, but targeted using contextual information. Google also disallows all interest-based audience targeting, including demographic targeting and user list targeting.
- **Restricted Data Processing:** When you activate restricted data processing, Google will limit how it uses data and will only serve non-personalized ads for California users subject to CCPA.
- **Limited ads:** Limited ads give publishers the ability to serve reservation ads in a limited way in the absence of consent for cookies or other local identifiers. If a publisher uses the IAB TCF v2.0 consent framework, we will attempt to serve an eligible limited ad when there is no consent for Purpose 1.



How EU user consent affects you

Under Google's EU user consent policy, you need to ask your users in the European Economic Area (EEA) and the UK for consent when showing personalized or non-personalized ads, for cookies and for analytics, and provide certain information about the way your app uses data. The requirements reflect the EU ePrivacy Directive, GDPR and equivalent UK legislation.

To collect consent you can use our IAB GDPR message or an alternative consent solution.

Choose the type of ads you want to show

You can choose from two ad options for your account for your users

Personalized ads

Select ad partners

Select ad partners to let them show ads on your sites or apps

Custom ad partners
4 partners

Check creatives for consent

You can include an additional check for consent for ad partners on creatives. Google will stop any creative that contains an ad partner that doesn't have valid user consent.

☑ Check reservation creatives for consent

Reservation creatives are associated with non-programmatic ads, including guaranteed and non-guaranteed.

Add custom ad partner URLs

Add URLs

Google Product Ad Manager | Ad Manager 360 | AdMob | AdSense

Platform App | Web

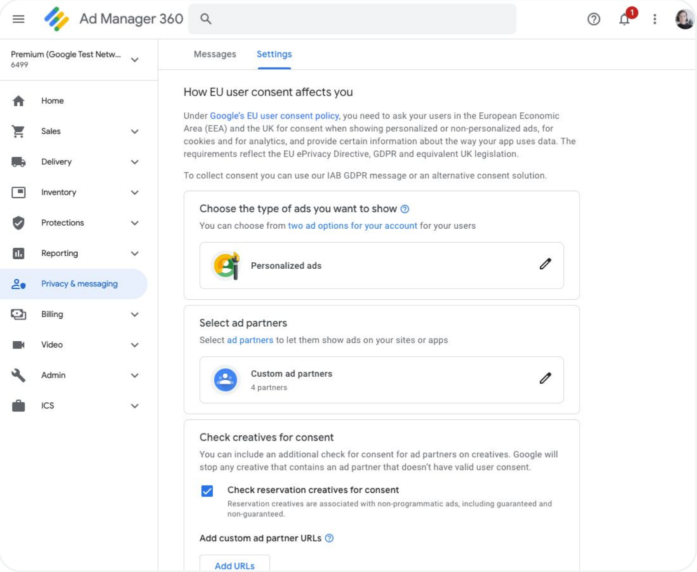
Demand Type Programmatic | Direct

Please note *Google tools do not guarantee regulatory compliance*

Ad Technology Provider Controls

Ad Manager provides publishers with controls to select which ad technology providers (ATPs) are allowed to serve and measure ads in the European Economic Area (EEA) and the UK, to support ad delivery, ad measurement, and other functions. This list of ATPs applies to programmatic demand and can be extended to reservations as well.

- **Reservation level controls:** Reservation creatives are associated with non-programmatic line items, including guaranteed (Sponsorship and Standard) and non-guaranteed (Network, Bulk, Price Priority, and House). Google will check for consent for any ad technology providers that you declare when determining whether reservation creatives are eligible to serve.
- **Real-time bidding (RTB) creative checking:** Opting into RTB creative checking allows Google to review your RTB creatives in Ad Manager to filter out RTB creatives where the vendor pixels don't contain the correct user consent (as detected by our systems).



How EU user consent affects you

Under Google's EU user consent policy, you need to ask your users in the European Economic Area (EEA) and the UK for consent when showing personalized or non-personalized ads, for cookies and for analytics, and provide certain information about the way your app uses data. The requirements reflect the EU ePrivacy Directive, GDPR and equivalent UK legislation.

To collect consent you can use our IAB GDPR message or an alternative consent solution.

Choose the type of ads you want to show

You can choose from two ad options for your account for your users

Personalized ads

Select ad partners

Select ad partners to let them show ads on your sites or apps

Custom ad partners
4 partners

Check creatives for consent

You can include an additional check for consent for ad partners on creatives. Google will stop any creative that contains an ad partner that doesn't have valid user consent.

☑ Check reservation creatives for consent

Reservation creatives are associated with non-programmatic ads, including guaranteed and non-guaranteed.

Add custom ad partner URLs

Add URLs

Google Product: Ad Manager, Ad Manager 360, AdMob, AdSense

Platform: App, Web

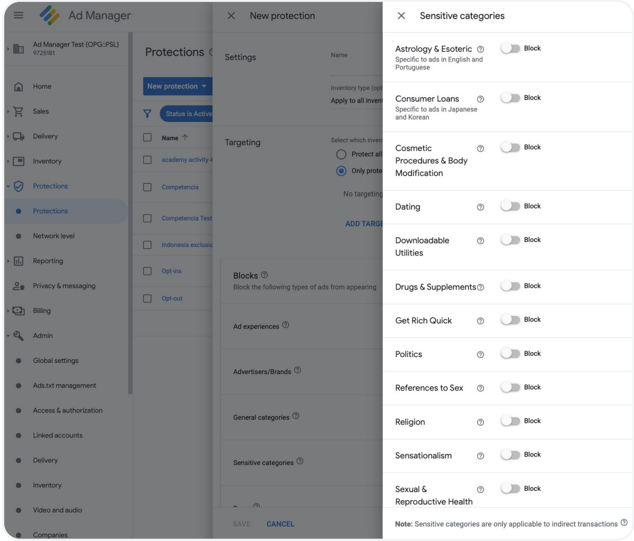
Demand Type: Programmatic, Direct

Please note *Google tools do not guarantee regulatory compliance*

Safeguarding Minors

In order to help support publisher compliance with COPPA, AADC, COADP, and other regulations that safeguard minors, Google offers multiple solutions to assist with ad depersonalization and creative filtering. Our solutions include **Tag for Child Directed (TFCD), Tag For Under the Age of Consent (TFUA), and Ad Content Controls.**

- **TFCD:** Mark your ad requests to be treated as child-directed, which includes ad depersonalization and creative filtering. The feature is designed to help facilitate compliance with the Children's Online Privacy Protection Act (COPPA).
- **TFUA:** Mark your ad requests to receive treatment for users in the European Economic Area (EEA), the UK, and Switzerland under the age of consent for restricted data processing using the TFUA tag. This feature is designed to help facilitate compliance with the General Data Protection Regulation (GDPR) and related child privacy regulations, such as the Age Appropriate Design Code (AADC).
- **Ad Content Controls:** Ad content rules help you control which types of advertiser categories are eligible to serve on your property. Specifically, these rules allow you to control ad experiences on content that may be for users under the age of 18.



Inventory type (opt
Apply to all invent

Select which inven
○ Protect all
● Only prote
No targeting

Blocks
Block the following types of ads from appearing

Sensitive categories

Astrology & Esoteric Specific to ads in English and Portuguese	Block
Consumer Loans Specific to ads in Japanese and Korean	Block
Cosmetic Procedures & Body Modification	Block
Dating	Block
Downloadable Utilities	Block
Drugs & Supplements	Block
Get Rich Quick	Block
Politics	Block
References to Sex	Block
Religion	Block
Sensationalism	Block
Sexual & Reproductive Health	Block

Note: Sensitive categories are only applicable to indirect transactions

Google Product Ad Manager | Ad Manager 360 | AdMob | AdSense

Platform App | Web

Demand Type Programmatic | Direct

Please note *Google tools do not guarantee regulatory compliance*

Section III

Privacy-minded Solutions

Overview

Our goal is to deliver durable solutions that make it easy for you to achieve your business goals while ensuring respect for user privacy preferences. Here are a few of the approaches we recommend publishers explore:

- 01. Privacy Sandbox
- 02. Contextual Audiences
- 03. Programmatic Direct Deals
- 04. AdSense for Search

Get to Know the Privacy Sandbox

Creating a More Private Internet

The Privacy Sandbox initiative aims to create technologies that both protect user privacy online and provide companies and developers tools to build thriving digital businesses. The Privacy Sandbox reduces cross-site and cross-app tracking while helping keep online content and services free for all.

Build new technology to keep information private

People should be able to enjoy their browsing and app experience without worrying about what personal information is collected, and by whom. The Privacy Sandbox technologies aim to make current tracking mechanisms obsolete, and block covert tracking techniques, such as fingerprinting.

Enable publishers and developers to keep online content free

Billions of people around the world rely on access to information on sites and apps. To provide this free resource without relying on intrusive tracking, publishers and developers need privacy-preserving alternatives for their key business needs, including serving relevant content and ads.

Collaborate with the industry to build new Internet privacy standards

The Internet is a source of information and engine of economic growth worldwide. Google invites members of the industry – including publishers, developers, advertisers, and more – to get involved and contribute to the development of better privacy standards for the Web and on Android.

Privacy Sandbox for the Web

Privacy Sandbox for the Web uses the latest privacy techniques, like differential privacy, k-anonymity, and on-device processing to enable functionality previously supported by third party cookies. Privacy Sandbox also helps to limit other forms of tracking, like fingerprinting, by restricting the amount of information sites can access so that your information stays private, safe, and secure.

Interest Based
Topics

Allows advertisers to show relevant ads based on topics (defined by browser) that demonstrate certain interests.

Remarketing
FLEDGE

On device auction to choose the most relevant ad including remarketing ads based on user browsing history.

Measurement
Attribution Reporting

Supports key advertiser measurement use cases ranging from event-level to aggregate-level reporting.

Jump to the Apps Section →

Privacy Sandbox on Android

On February 16, 2022, Google announced the extension of the Privacy Sandbox initiative to Android. Android intends to fundamentally advance privacy for the mobile app ecosystem while supporting key advertising use cases, and offer users access to their favorite apps.

The web and mobile apps rely on fundamentally different technologies, but there are similarities in the ways advertising supports the web ecosystem and the ecosystem of apps.

The development, testing, and adoption of these technologies is expected to span at least two years. Android will share more details as they become available.

Google's Ads teams are supportive of Android's vision and will engage with Android and the apps ecosystem to offer feedback on durable, privacy-safe solutions that continue to make advertising available as an effective means to support and grow their business.

Getting Involved with the Privacy Sandbox

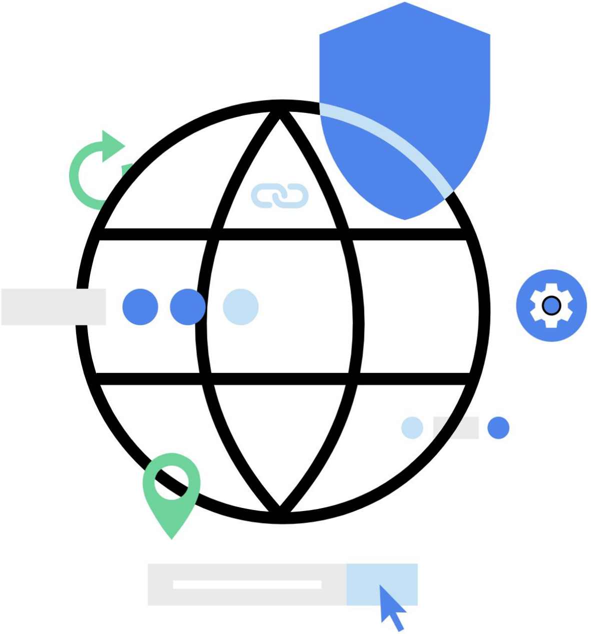
In many cases, publishers will not need to directly adopt the privacy-preserving technologies from the Privacy Sandbox, as their ad tech providers are likely to be implementing solutions on their behalf.

Stay Informed

Visit the Privacy Sandbox website to learn more about the current proposals for both Web and Android.

Give Feedback

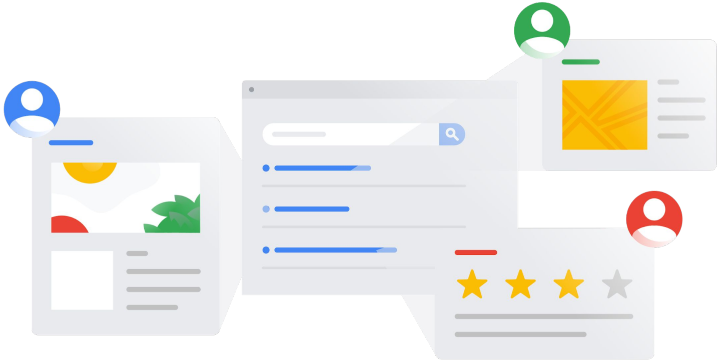
Provide your feedback directly to the Chrome and Android teams to help shape the proposed APIs.



Contextual data helps connect advertisers with interested audiences

Contextual data is one of the oldest and most accessible ways for publishers to create compelling privacy-centric audience lists for advertisers. In practice, it's very simple. For example, when you categorize articles or videos as content about "personal fitness," it's safe to assume that advertisers looking to reach fitness enthusiasts would be interested in placing ads on that content.

While on the surface this seems straightforward, sophisticated publishers invest a lot of time adding additional granularity to their contextual signals, which in turn adds value and creates more opportunities for their inventory. To use the example above, if you create additional sub-categories for "personal fitness" content like "yoga," "cycling," or "running," advertisers can further personalize their messaging and you can charge a higher CPM for the more specific audiences.



Use Key-values to execute your contextual targeting strategy

Key-values are extra parameters that you can add to your ad request to better specify targeting criteria. Key-values help your advertisers and buyers reach their intended audience or demographic, and add value to your offerings when negotiating campaigns.

Full Guide

To get started with key-values:

1. Develop a plan on how best to use key-values
2. Add new key-values in your network according to your plan
3. Include key-values in Google Publisher Tags (GPT) as you tag webpages or apps
4. Target key-values in line items, proposal line items, and more

Google Product	Platform	Demand Type
Ad Manager Ad Manager 360	App Web	Programmatic* Direct

**Only available for Programmatic Direct deals*

Programmatic Direct Deals

In a privacy-forward environment, Programmatic Direct can help publishers increase the value of their inventory by leveraging contextual signals and first-party data.

Programmatic direct deals for 1:1 trusted relationships

Programmatic Direct automates the negotiation and sales of your direct-sold inventory through both Programmatic Guaranteed and Preferred Deal campaigns in Ad Manager.

Programmatic Guaranteed: You and the buyer negotiate a price and terms for inventory that's reserved (guaranteed) for that buyer. Inventory is designated only for that buyer at that price.

Preferred Deal: You and the buyer negotiate a price and terms for inventory that the buyer can optionally buy. The buyer has an initial, or "preferred," opportunity to bid at the negotiated price when there's an ad request for the inventory.

Programmatic Direct expands on the promise of programmatic advertising to deliver more value to both advertisers and publishers by allowing them to implement direct reservation-style buys more easily than ever before.

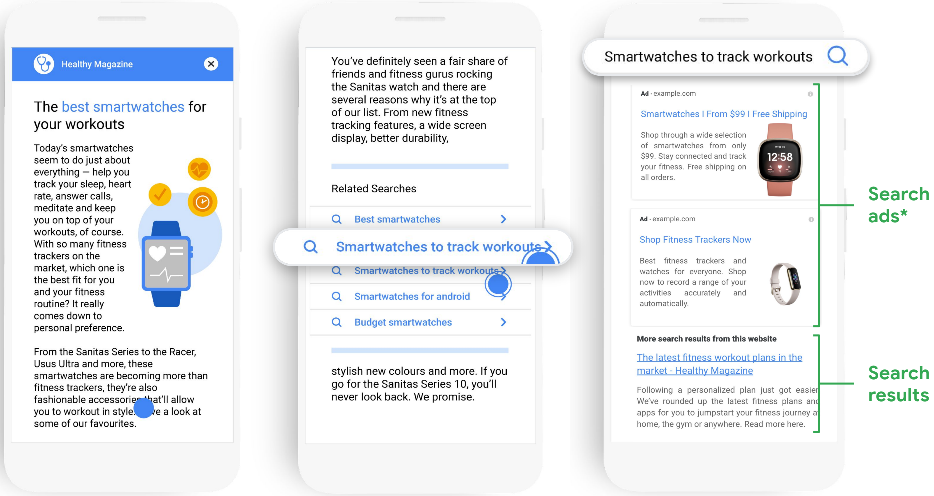
Google Product Ad Manager | Ad Manager 360

Platform App | Web

Demand Type Programmatic

AdSense for Search

Search ads perform well, even without personalization. AdSense for Search (AFS) targets keywords, not users.



Healthy Magazine ✕

The best smartwatches for your workouts

Today's smartwatches seem to do just about everything — help you track your sleep, heart rate, answer calls, meditate and keep you on top of your workouts, of course. With so many fitness trackers on the market, which one is the best fit for you and your fitness routine? It really comes down to personal preference.

From the Sanitas Series to the Racer, Usus Ultra and more, these smartwatches are becoming more than fitness trackers, they're also fashionable accessories that'll allow you to workout in style. ve a look at some of our favourites.

You've definitely seen a fair share of friends and fitness gurus rocking the Sanitas watch and there are several reasons why it's at the top of our list. From new fitness tracking features, a wide screen display, better durability,

Related Searches

- Best smartwatches
- Smartwatches to track workouts
- Smartwatches to track workouts
- Smartwatches for android
- Budget smartwatches

stylish new colours and more. If you go for the Sanitas Series 10, you'll never look back. We promise.

Smartwatches to track workouts

Ad · example.com

Smartwatches I From $99 I Free Shipping

Shop through a wide selection of smartwatches from only $99. Stay connected and track your fitness. Free shipping on all orders.

Ad · example.com

Shop Fitness Trackers Now

Best fitness trackers and watches for everyone. Shop now to record a range of your activities accurately and automatically.

More search results from this website

The latest fitness workout plans in the market - Healthy Magazine

Following a personalized plan just got easier We've rounded up the latest fitness plans and apps for you to jumpstart your fitness journey a home, the gym or anywhere. Read more here.

1. User visits an article on the site
2. User clicks on a search term in Related Search unit to explore more.
3. User views relevant search ads and search results.

1 Diversify ad revenues with the help of Related Search on your content pages

Related Search can help your users explore more content on your site and let you diversify ad revenue without requiring ads personalization.

2 Generate incremental revenue by monetizing your search results pages

Adsense for Search (AFS) uses the user's search query to deliver highly targeted, relevant ads.

3 High-performing search ads

Search, shopping, and other visual formats perform strongly on search pages. AdSense for Search (AFS) enables you to access search ad budgets.

Google Product AdSense for Search | **Platform** App Web | **Demand Type** Programmatic

Search ads do still need cookies and cookie consent.

Section IV

Building First-party Audiences

Overview

Google is investing in several solutions to make it easier for publishers to collect, measure, and activate first-party data. Learning more about first-party data can help you increase value for users and buyers.

- 01. Defining First-party Data
- 02. Growing Your Audiences
- 03. Monetizing Audiences
- 04. Identifiers for Programmatic

Defining First-party Data

“First-party” refers to the 1:1 direct relationship between two parties. First-party data is the information that you learn through those direct relationships with people who visit and engage with your site or app.

There’s a wide range of the types of information you may learn from visitors. For example, it could be an email address that someone provides when they sign up for a newsletter. Or, it could simply be understanding which pages someone has visited on your site.

Even in a landscape of evolving user expectations and regulations, publishers still need to know who their audiences are, add value for users, and package their inventory in creative and valuable ways for advertiser clients. As users continue to embrace different ways of engaging with, paying for, and consuming publisher content, there are more opportunities than ever to form meaningful relationships.

Adding value for users to create first-party data

When your audiences give you permission to use their data, they expect to receive something in return. Creating a fair value exchange by enhancing their experiences is critical to growing and developing deeper user relationships. The primary value most publishers provide their users is original content that’s entertaining, informative, or helpful. There are several ways that publishers can connect users with their content — while also building out their first-party audience data.

Defining First-party Data

The difference between first- and third-party data

The ad industry is investing more in privacy-forward first-party data, and moving away from third-party data. The key differences between the two are explained below:

Who collects the data

First-party data is captured and stored by a website or app owner. Third-party data is commonly collected across multiple sites that aren't owned by the businesses doing the collecting.

Permissions

With first-party data, people provide businesses they have direct relationships with permission to use their data, and the businesses are responsible for how the data is used. In contrast, third-party data can be collected and used, often without people fully knowing how their data is being activated.

Relevant privacy laws apply to first- and third-party data alike. That's why it's so important to have clear privacy policies in place, so users know exactly what data they're sharing along with its intended use.

Growing Your Audiences

70% of publishers believe that their ability to activate first-party data will provide a significant advantage in the privacy-centric ecosystem.

See the research

Source: Deloitte Study - Future-proofing ad sales growth through first-party data

Case Study

See how the Wall Street Journal is activating first-party data to achieve their desired performance.

Read more

Most publishers, even smaller ones, can easily implement strategies to start growing their first-party data. In exchange for additional content or functionality, many publishers are encouraging consumers to sign in.

Some publishers even create or acquire entirely new businesses, such as loyalty programs, credit card offerings, or online stores, to fill in their data gaps.

Monetizing Audiences

Leverage your own first-party identifiers with PPID

Google Ad Manager publishers with existing first-party datasets can use Publisher Provided Identifiers (PPIDs) to create encrypted identifiers, build audiences, and deliver ads to first-party audience segments. PPIDs are set and controlled by you and will continue to work even when third-party identifiers like 3P cookies are no longer supported.

Publisher provided identifiers (PPID) are a privacy-forward solution as they:

- Must be hashed, and the underlying data is not accessible by Google. Only you know their meaning.
- Must not contain personally identifiable information (PII).
- Are specific to individual Ad Manager networks, are not shared with other publishers, and are not joined with any other identifiers.

Case Study

See how Pandora is successfully monetizing their first party data.

Read more

When considering developing PPIDs, keep these steps in mind:

1. Determine what first-party data you have available.
   - Publishers that have user sign-in data may be able to develop PPIDs based on that user data. Examples include usernames and user IDs.
   - For those without user sign-in data, PPIDs may also be developed using publisher first-party cookies, which deploy based on user visits. They can be based on a variety of attributes such as visit frequency, content visited, and checkout cart activity.
2. PPIDs are passed to Ad Manager with each ad request using your existing GPT tags, GMA SDK, or IMA SDK. Contact your Google Account Manager for activation.

Google Product Ad Manager 360 | **Platform** App Web | **Demand Type** Direct

Monetizing Audiences

Build and manage first-party segments with Audience Solutions

PPIDs can be used to create and manage first-party audience segments in Ad Manager 360 Audience Solutions.

Once a PPID-based audience list is present within Ad Manager 360 Audience Solutions, reservations and programmatic deal line items can be targeted to those first-party audiences in order to improve ad performance for advertisers, and ad relevance for users. Individual PPIDs can then be passed into Ad Manager 360 with each ad request, which Ad Manager 360 uses to check against any first-party audience lists that are present.

In this way, PPIDs are the key that allows a given ad request to be matched against PPID-based audience lists.

PPIDs are also used by Ad Manager 360 for core ad server functions controlled by you, including:

- Frequency capping for reservations
- Sequential ad rotation for reservations
- Creative rotation for reservations

Google Product Ad Manager 360 | **Platform** App Web | **Demand Type** Direct Deals

Publisher Provided Signals

Use Publisher Provided Signals (PPS) for contextual signaling & to communicate first-party attributes

Publisher Provided Signals (PPS) is a new feature, currently in beta, to help increase programmatic monetization. PPS will enable publishers to communicate their first-party audience attributes and contextual data to programmatic buyers by using standardized taxonomies.

We are working with partners to incorporate industry standards into publisher provided signals. As a first step, we are integrating the IAB Tech Lab's Seller Defined Audiences.

To get started with Publisher Provided Signals (PPS):

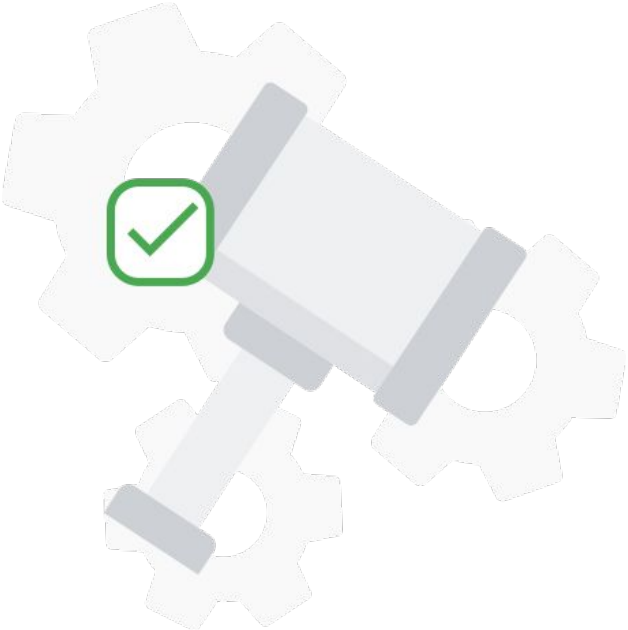
- Publishers or their DMP or data vendor partners segments their audience into cohorts and categorize using supported standardized taxonomies
- Publisher includes taxonomy categories (like demographic data, interests, or purchase intent), and/or segment IDs in a bid request
- Buyer reads categories/segment IDs and decides whether to bid.

Google Product	Ad Manager Ad Manager 360	**Platform**	App Web	**Demand Type**	Programmatic Programmatic Direct

Identifiers for Programmatic

Identifiers are also very important when selling ad inventory programmatically. Programmatic bidders (i.e. DSPs) receive bid requests in real time, evaluate the ad impression, and bid accordingly. When third-party cookies or IDs are blocked or restricted, buyer-set frequency-capping functionality is impacted which may result in users experiencing the same ad repeatedly. Because of this, some advertisers may decide to exclude certain media altogether if no identifier is present, and publishers may earn less revenue as a result.

Additionally, presence of an identifier in programmatic bid requests allows bidders to potentially develop an understanding of a user's interests based on repeated exposure to the same identifier from a publisher over time. This learning can be used to serve more personalized ads to users on the publisher's sites/apps, improving ad performance and user experience.

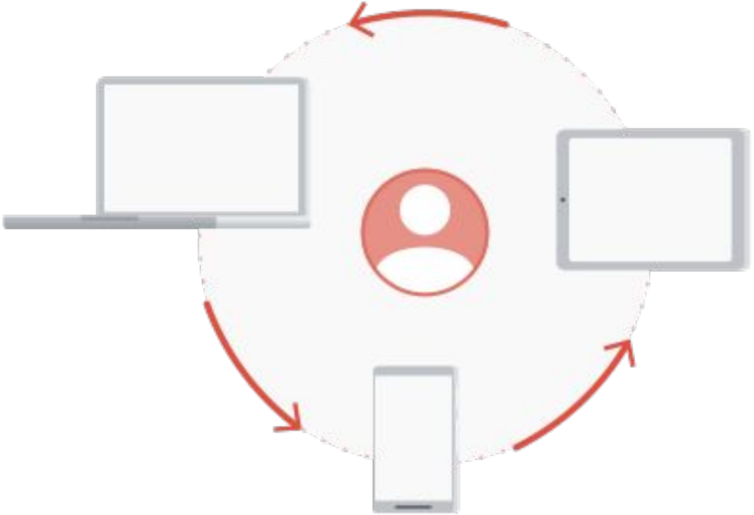


PPID for Programmatic

When enabled by you within the Ad Manager 360 UI, PPIDs that are present on a given ad request may be utilized by Google programmatic demand to support buyer frequency capping and interest-based ads personalization on your programmatic traffic, when third-party cookies or device IDs aren’t available.

It's important to note that before sharing PPIDs with Google demand, Ad Manager turns them into per-publisher partitioned IDs, so users cannot be identified across other publishers’ sites and apps. A PPID shared from your Ad Manager network will never match a PPID shared from a different Ad Manager network, which limits the use of the ID to within the same Ad Manager network.

In sum, when sharing your PPIDs with Google programmatic demand, buyer frequency capping and interest-based ads personalization can be used to inform bidding on your inventory only, potentially increasing your programmatic revenue, and improving ad performance and user experience.



Google Product Ad Manager 360 | **Platform** App Web | **Demand Type** Programmatic

*DV360 & Google Ads Only, See Secure Signals slide for a solution for Authorized Buyer & Open Bidders

Automated First-Party Identifiers

Enabling first-party identifiers for publishers of all sizes with same app key

In cases where mobile Ad IDs are not available same app key provide a frictionless and effective way to personalize ads in a privacy-first way.

Same app key helps publishers serve relevant ads on iOS without tracking users across third party apps by using data collected from your apps, such as information about ad interactions users take inside your app, to improve ad relevance.

What is same app key?

- First-party IDs set on your app by Google
- Privacy-first, scoped to your app, not shared with other publishers, and are not joined with any other identifiers
- Provides optional controls for publishers to disable the use of same app key for programmatic ads personalization

Google Product Now Available: AdMob
Coming Soon: Ad Manager

Platform App

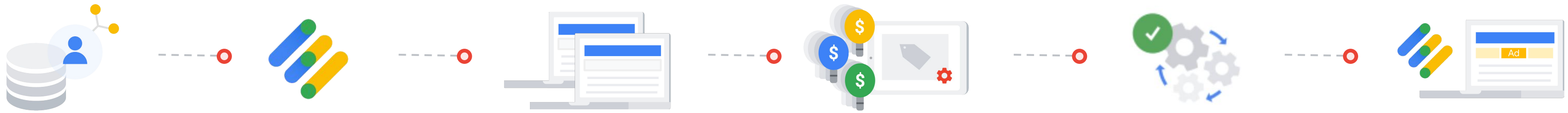
Demand Type Programmatic*

*DV360 & Google Ads Only, See Secure Signals slide for a solution for Authorized Buyer & Open Bidders

Secure Signals

Respecting direct relationships with secure signals

We are building a feature to enable publishers to securely share signals with Authorized Buyers and Open Bidders via Ad Manager. The signals passed through our systems will not be readable by Google, preserving the confidentiality of the relationship between the publisher and the buyer.



1. Publisher implements ID Provider solution and adds related code to their site
2. From the Ad Manager UI, publisher enables chosen partners to collect signals which are passed to Ad Manager
3. User visits publisher website
4. Ad Manager routes the secure signals from the publisher to the bidders the publisher works with as part of the bid request
5. Bidders send bid responses back to Ad Manager, taking the secure signals into account
6. Ad Manager selects winning candidate and displays ad

Google Product Ad Manager · Ad Manager 360 · AdMob | **Platform** App · Web | **Demand Type** Programmatic*

*For Authorized Buyers and Open Bidders only. Not available for DV360 or Google Ads.

Section V

Adapting To App Platform Changes

Overview

Google's approach to privacy extends across all platforms and devices. While privacy on the web has received significant attention in recent years, it's important for publishers to understand the current apps landscape and prepare for what's to come.

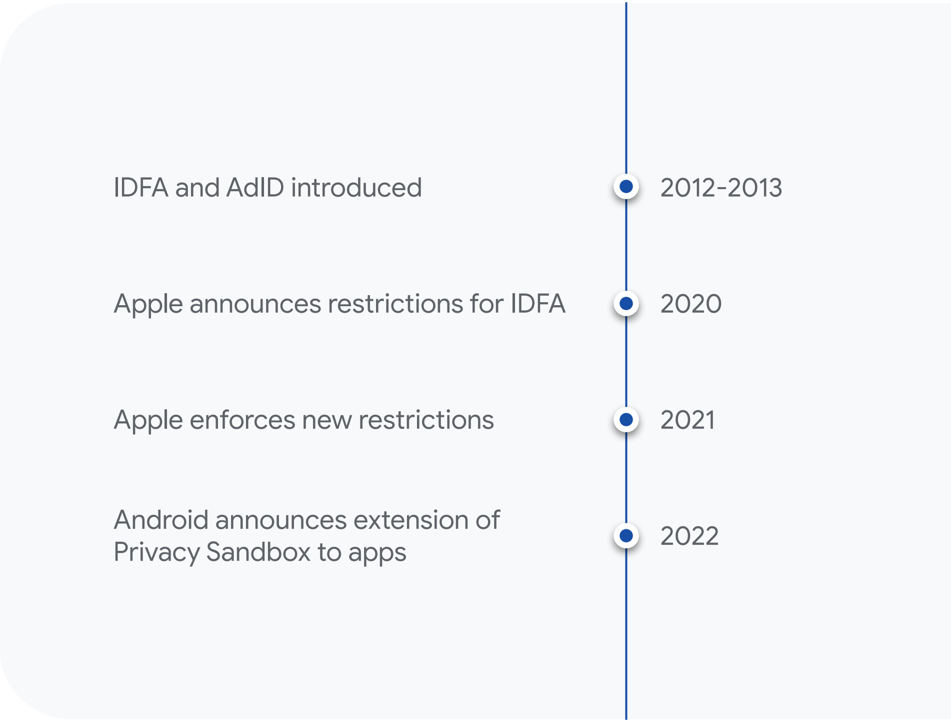
- 01. Platform Changes
- 02. iOS Solutions
- 03. Android Solutions

Platform Changes

Technology changes are fundamentally altering the foundations of the digital ads industry

Increased user expectations are driving both additional regulations and tech changes that restrict user identifiers:

- Regulatory scrutiny over how businesses collect and use consumer data is increasing globally. Mobile operating systems are shifting away from mechanisms that track users across sites by restricting third-party cookies as well as mobile ad identifiers. The shifting landscape is phasing out cross-web and app identifiers used for marketing and measurement.
- At the same time, technology platforms, such as mobile operating systems, have announced or implemented new policies to change the way user data is collected, shared, and measured.

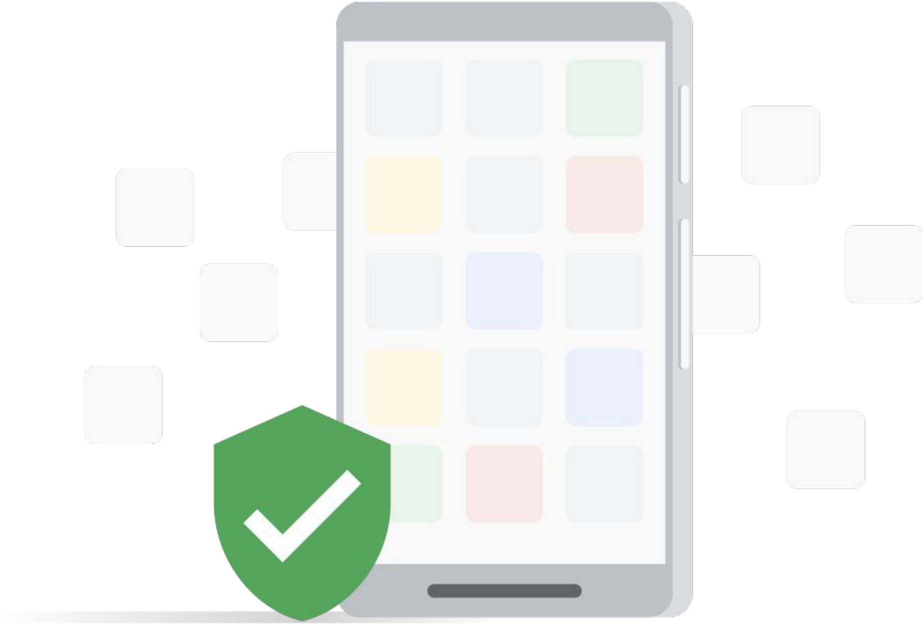


IDFA and AdID introduced	2012-2013
Apple announces restrictions for IDFA	2020
Apple enforces new restrictions	2021
Android announces extension of Privacy Sandbox to apps	2022

iOS Solutions

In June 2020, Apple announced an update to iOS 14 requiring apps to ask users for permission to access Apple's identifier for advertisers (IDFA) through a prompt called App Tracking Transparency (ATT) framework.

- These changes will reduce visibility into key metrics that show how ads drive conversions, and will affect how advertisers value and bid on ad impressions.
- As such, app publishers have seen a significant impact to their Google ad revenue on iOS.
- Read on for recommendations on how you can update your app for iOS 14+ and help protect your ad revenue.



iOS Solutions

Keep your SDK Updated

Keep your GMA SDK up-to-date to take advantage of the latest features and functionality, including SDK Instance ID and Same App Key. (🔗 AdMob, 🔗 Ad Manager)

Apple's SKAdNetwork

In order for advertisers to identify your app as a valuable source of their ads traffic, you will need to configure SKAdNetwork with Google's Network key. (🔗AdMob, 🔗Ad Manager)

ATT Messaging

Determine if ATT is right for your app. Google's 🔗 Privacy & messaging tab offers an option to create and manage the ATT prompt and optional explainer messaging

Mediation Groups

For iOS apps, you can now create distinct mediation groups for ad requests with and without an Identifier for Advertisers (IDFA). (🔗AdMob, 🔗Ad Manager)

Google Product Ad Manager · Ad Manager 360 · AdMob · AdSense | **Platform** App | **Demand Type** Programmatic · Direct

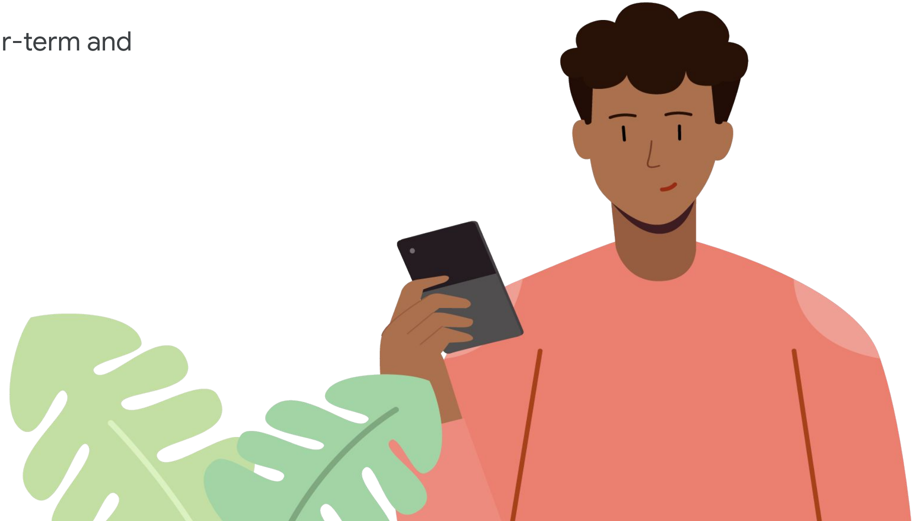
Android Solutions

In July 2021, Google Play and Android announced policy updates to bolster privacy and security to make Google Play a safer and more trustworthy experience for developers and consumers.

In February 2022, Android announced the Privacy Sandbox on Android, a multi-year collaborative industry effort intended to fundamentally advance privacy for the ecosystem, without sacrificing key ads functionality and without putting access to ad-supported apps at risk.

In this section, we aim to help you understand both the near-term and long-term privacy efforts happening on Android.

Just like the entire industry, Google Ads will take time to evaluate the proposals and test how we may incorporate these solutions into our own products. So while there are no actions for you to take today, we encourage you to familiarize yourself with the high-level approach Android is taking and, if you're interested, sign up for updates on developer.android.com.



Android Solutions

In 2021, Google Play and Android announced several new policy updates and technical changes to enhance privacy and security.

Android Update	Recommended Action
Introduction of Data safety section in Google Play console and the requirement for new app submissions and app updates to include data disclosures by Q2 2022.	Consult GMA SDK (AdMob, Ad Manager) and IMA SDK guidance to update Play Console information.
Updates to the Google Play Families Policy Requirements. If one of the target audiences for your app is children, your app must not transmit certain identifiers (including the advertising ID) for children or users of unknown age.	Developers who have apps with children audiences should update SDKs to support updated TFCD and TFUA behavior.
As part of the Google Play services update in late 2021, the advertising ID will be removed when a user opts out of personalization using advertising ID in Android Settings.	Developers who directly use AdID today for essential, non-Ads use cases are encouraged to adopt the app set ID (more information below). Apps targeting Android 13 will need to declare a Google Play services permission in the AndroidManifest.xlm file in order to use Advertising ID. Developers targeting Android 13 should update their SDKs or manually update their manifest.
A developer preview of app set ID for essential use cases such as analytics or fraud prevention.	To retain the use cases like fraud or analytics for users opting out from Advertising ID, developers should adopt updated SDKs to support app set ID.

For more information on the Privacy Sandbox, visit the Privacy Minded Solutions section →

Extending the Privacy Sandbox initiative to Android

On February 16, 2022, Google announced the extension of the Privacy Sandbox initiative to Android.

Android intends to fundamentally advance privacy for the mobile app ecosystem, while supporting key advertising use cases, and offer users access to their favorite apps.

Android's Approach

New solutions for ads use cases

Privacy-preserving APIs that don't rely on cross-party identifiers and limit user data sharing.

Reducing covert tracking

Technologies that reduce the potential for undisclosed data collection.

Working closely with the industry

Engagement and feedback to shape designs that improve user privacy and support the ecosystem.

THIS WILL BE A MULTI-YEAR COLLABORATIVE EFFORT

Key Takeaways

01. Expect change, as the landscape will continue to evolve

02. Start preparing for the future today

03. Develop a comprehensive plan and privacy strategy

04. Partner with legal teams and partners on global regulations

05. Invest and explore multiple privacy-minded solutions

06. Grow and activate your first party data

07. Tap into Google resources for trainings and additional guidance

Thank you

Google