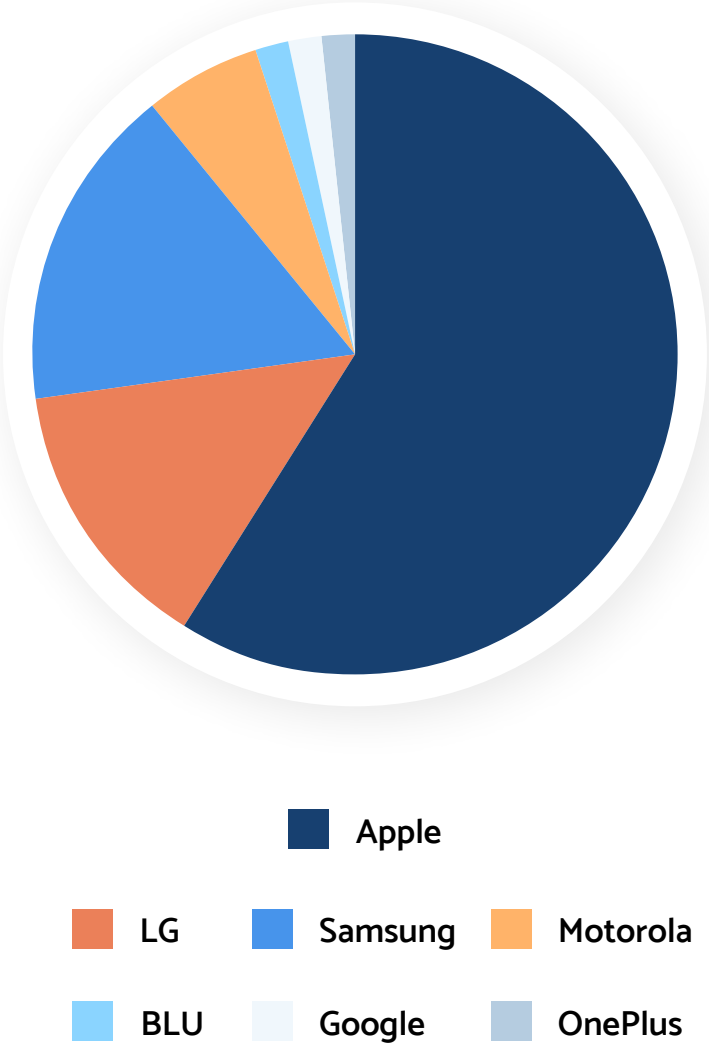


Fig 1 - An example of mobile devices that drive lead inquiries reported from Google analytics. For our clients, the range is between 53 - 76% of mobile inquiries coming from Apple devices.

The impact to mobile advertising is dramatic to say the least with Apple devices averaging **64% of all mobile generated leads** for our clients alone.

Enrollment Resources
Innovations in Enrollment Management

A Digital Marketing Reset As Privacy Takes Center Stage

Recently, digital marketers and the online advertising platforms they use have been faced with a challenging loss of data. New cookie tracking restrictions went into effect in April of this year for Apple devices that were prompted by privacy concerns around personal data use.

This isn't the first time Apple took the initiative to block their users from being tracked. However, the IOS 14 update in April has impacted every digital advertising network globally and is reshaping how ads are delivered online.

In comparison to other mobile devices, that is a big data gap to fill and has a cascading effect on how Artificial Intelligence (AI) is used to deliver personalized ads across every network.

For digital marketing, it's a massive shift in the machine learning foundation. The complicated networks of data sharing for ad perstonalization that most advertising AI has been built upon have some major blackouts in their data.

A Cookie Primer - Why the Apple IOS Update Is Making Waves

There are two types of cookies that track user behaviour. First-party cookies are directly stored by the website the user visits. These allow website owners to collect data which works to create better user experiences.

Any first-party data is minimally affected by the IOS 14 update and will continue to report data. First-party data can be classified as:

- Traffic generated to your website
- Keyword search traffic (paid and SEO)
- CRM data collected from your prospects

It is third party cookies that are problematic.
Third-party cookies are created on websites external to your own and track user behaviour across their entire browsing experience and app use.

These cookies contain personal identifiable information, which is stored and then often resold to aggregate ad networks. The ad networks use this information to create highly targeted ads aimed at individual users.

This is where certain ad targeting can become invasive and has precipitated Apple's push for privacy and data protection, and the introduction of US legislation across multiple states which is expected to be brought forward in 2023.

Apple now requires apps on their devices to gain permission from their users before using their information for advertising. This implementation will prompt users with a discouraging message warning them about the information used to track them, requiring agreement (opt-in) before they can be targeted by advertisers.

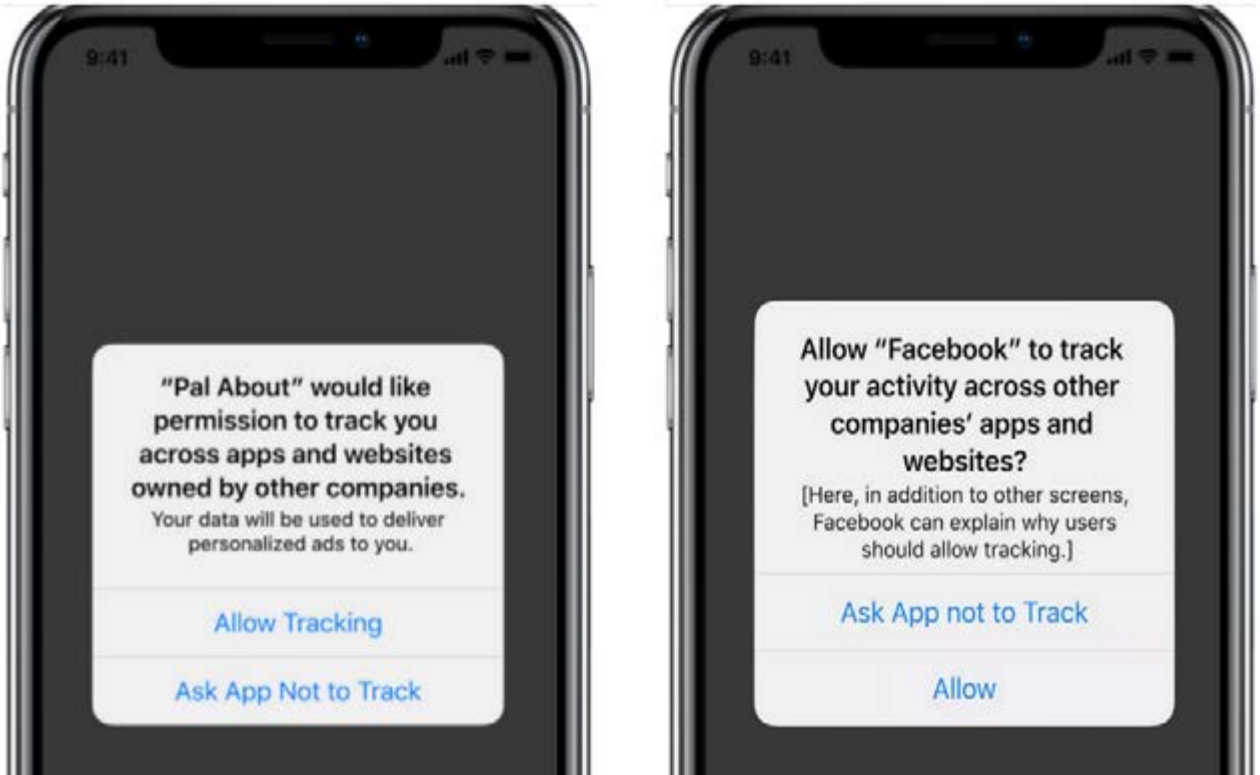


Fig 2 - Examples of notifications Apple app users may see with the IOS 14 update.

Image source - Seer Interactive.

Since the iOS 14 update launched in April, speculations are that 85% of Apple users have not opted-in to being tracked.

The foundation of machine learning in advertising was built on third-party cookie data. If the machine is missing data, it will start to make decisions that may not be reflective of actual performance. This can upset the optimization of bids and ad auctions, resetting the algorithms of what may have historically been a strong campaign.

As advertisers lose visibility on what is driving the best return, they will begin shifting their budgets to less volatile networks such as search engine marketing.

Online Advertising Most Impacted By This Privacy Update

The biggest disruption for digital advertisers are on the following networks currently dependent on third-party cookies to deliver relevant ads:

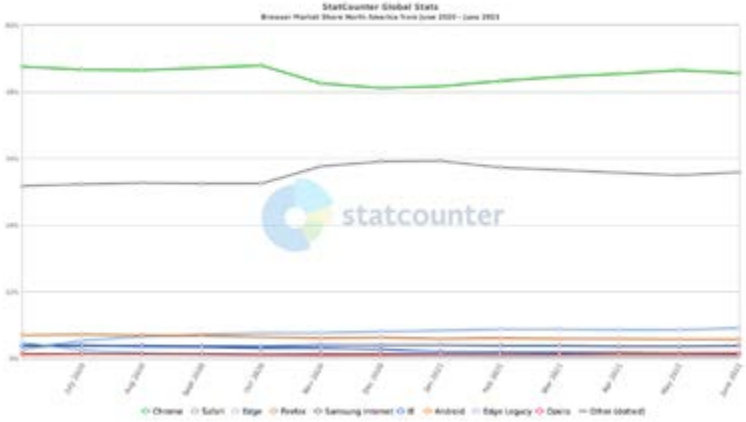
- Display networks
- YouTube
- Social ad platforms
- Remarketing
- Programmatic advertising
- Geofencing

Blocking third-party cookie data on these dominant ad networks has:

- Reduced the ability to follow previous visitors on Apple devices with ads while they browse
- Limited iOS users from seeing the same ad over-and-over in a certain time period
- Disrupted the use of website data to build effective similar audiences for scale
- Created gaps in lead conversion data used to define the best course of action for performance

Apple is a first mover in the conversation of privacy protection for internet users with their iOS 14 update. However, they are not the only platform making this transition.

Google has announced they will also be blocking third-party cookies on their Chrome browser in the near future. As a dominant browser in North America, many advertising networks reliant on shared third-party data gain significant insights on user behavior for ad targeting.



There Are New Privacy Safe Solutions on the Horizon

Every online ad network has had to resuscitate their machine learning models. This requires investment in new approaches to privacy safe performance measurement and targeting.

New best practices are emerging to help close the data gap and maintain the data-driven performance advertisers have come to expect in their online campaigns.

In our recent meetings with the Google Measurement team, they spoke of two features currently in BETA:

1. Enhanced conversion for Google Ads
2. Server-side tracking in the Google cloud

Google emphasized that these new technologies will require the use of first party data and involve changes to your tracking process.

The Enhanced Conversion Model

To fill the gaps, enhanced conversion tracking for Google Ads will combine cookie data and email addresses collected from form submissions.
In order for this feature to work, you will need to use Google Tag Manager and make some adjustments to your tracking codes. Currently in BETA, it is expected that Enhanced Conversions will be available in a few months.

Server-Side Tracking With Google Tag Manager

Server-side tracking gives you more control over what data Google and other third parties collect about your visitors.

Current technology uses tracking tags from third parties on your website and these tags collect whatever they want. With server-side tracking, this data is processed by a server you control before sending to third parties. This not only enhances privacy and compliance, but also allows for data enrichment and future browser compatibility.

The feature is currently available but is in its very early stages of development so keep an eye out for updates on this new product.

Recommendations To Prepare For Future Tracking Models

To ensure our clients are leading in their digital marketing strategy, we have a number of initiatives in process. At its core, the fundamentals of tracking your website and landing page traffic must be in place for future technologies to work.

1st Party Measurement

Ensure that with any user data you are collecting, as with Google Analytics, Google Ads, and/or Facebook Ads, tracking codes are not placed directly on your website pages.

If you do, performance reporting to your advertising platforms will be seen as third-party cookies and will be blocked by Apple devices, Safari, Firefox and soon Chrome browsers.

Use a code container tool like Google Tag Manager to house all your tracking codes. Using a container tool transforms your tracking to first-party data and bypasses a number of the third-party cookie issues.

Google's emerging conversion modeling technology will require the use of Google Tag Manager in order to fill any gaps in measurement.

Facebook and other social platforms currently rely on importing your lead data into their ad platform to track lead performance.

Track Advertising in Your CRM

If you are a PPC client, we capture all the relevant advertising details for you in Virtual Advisor.

For schools running their own advertising, it is recommended to import advertising data into your CRM. This will give you better transparency on which networks and campaigns are providing the enrollments. Some examples of data you can capture and import:

- Keywords
- Campaign IDs
- Ad Group IDs
- Networks

Prepare to Update Your Digital Technology

The responsibility of privacy and security of users' data is being placed directly on the domains who collect this data. Apple's update is really a canary call to bigger shifts coming in the near future to ensure the lives behind the screens are protected.

The more we can transition away from browser-based cookie tracking and place data measurement security in the hands of website owners, the better it will be for everyone.

Server-side technology will become the gatekeeper, allowing advertisers to turn their data into first-party tracking and remove the issues around third-party blocks.

In digital marketing, as the data pools shrink from the loss of third-party tracking, the reliance on first-party data from website and app owners becomes the new paradigm. Server-side tracking will play a dominant role in this transition.

REFERENCE RESOURCES

Worldwide Opt-in Tracking
https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/

Legislation coming 2023
https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Server-side tracking
https://www.simoahava.com/analytics/server-side-tagging-google-tag-manager/

About Enrollment Resources

Our Mission is to “Pursue the Truth” Our core mission in business is to find the most profitable, ethical, and effective avenues of improving enrollment management performance. We are sticklers for testing, and are constantly challenging the status quo to find best practices that can guide our and our clients’ success.

Learn more at www.enrollmentresources.com