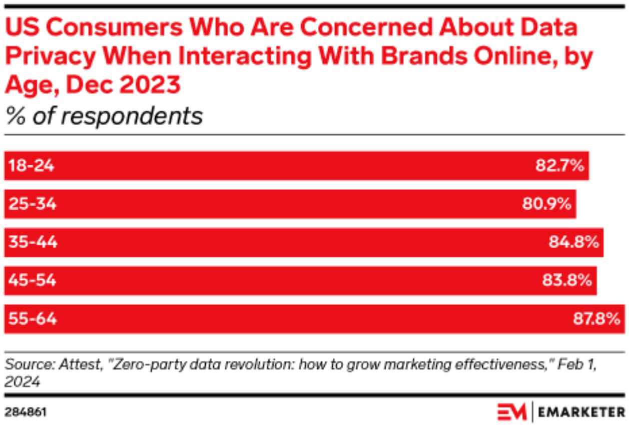
EMARKETER

Sara Lebow

3 non-cookie threats to ad targeting: VPNs, Apple's Private Relay, and ad-blockers

Article

At least 80% of US consumers across age groups are concerned about data privacy when interacting with brands online, according to December 2023 data from Attest. And more than half of consumers would stop interacting with companies that have bad reputations around data or don't allow them to opt out of tracking, per Q2 2024 data from Publishers Clearing House. Here are three non-cookie threats to advertising and information about what advertisers can do to stay visible.



US Consumers Who Are Concerned About Data Privacy When Interacting With Brands Online, by Age, Dec 2023

% of respondents

Source: Attest, "Zero-party data revolution: how to grow marketing effectiveness," Feb 1, 2024

1. VPNs

Some 66% of people who use VPNs use them to help protect personal data, according to Forbes Advisor.

VPNs don't remove ads, but they can disrupt location-based advertising by hiding IP addresses, confusing ad measurement and targeting. That presents a potential issue for connected TV (CTV) in particular, which uses IP addresses to associate devices in the same household.

Some VPNs come with ad-blockers. Mullvad, which has made a huge out-of-home ad push recently, features ad-blocking and content-tracking functions. Even though the VPN itself may not prevent users from seeing ads, subscribers to its service may use these ad blockers.

Mullvad and services like it cost money, which means consumer adoption likely isn't as high as free VPNs. The threat these VPNs pose to advertising is "minimal, but not negligible," said our analyst Evelyn Mitchell-Wolf.

2. Apple's Private Relay

Apple's Private Relay, a feature that obfuscates email and IP addresses in Safari, is another not yet widely adopted technology that threatens ad targeting.

The feature comes with iCloud+, which costs as little as $0.99 per month in the US. If Apple were to implement Private Relay by default into an iOS update, the feature could be a “nuclear option” for the Conversion API (CAPI) model, as noted by media strategist Eric Seufert in a Mobile Dev Memo article cited by AdExchanger.

CAPI is a vital part of Google’s and Meta’s strategies following Apple’s AppTrackingTransparency updates in 2021, so if Apple were to drop such an update, it could also deliver a blow to two of its biggest competitors.

3. Ad blockers

The threat ad blockers pose is more obvious than the above two examples—they block consumers from seeing ads. Some 31% of US adult consumers use ad blockers, according to March 2023 data from Tinuiti.

Publishers are taking measures to overcome ad blockers. YouTube has led the charge in video advertising, testing new ways to keep ad blockers from impacting its content. And publishers can mandate or encourage users white-list their websites and allow ads, though that often involves publishers paying ad blocker companies to allow ads to be seen.

What marketers can do: It’s probably impossible to divorce your ad strategy from IP and email addresses, or from display and video ads entirely in the case of ad blockers. But marketers can make sure they’re taking a diversified approach to avoid one single threat toppling their entire approach.

- Take advantage of contextual targeting to deliver ads within relevant content.
- Leverage first-party purchase data by advertising with retail media networks or publishers with retail media partnerships.
- Look to native advertising to integrate messaging with content.
- Work with influencers to reach audiences that opt in to seeing their content.

This was originally featured in the EMARKETER Daily newsletter. For more marketing insights, statistics, and trends, subscribe here.