URL GENIUS

Whitepaper

Surveillance Marketing

How Apps Enable Third-Party Tracking as Marketers Shift to First-Party Strategies

New Privacy Policies but Same Old Tracking?

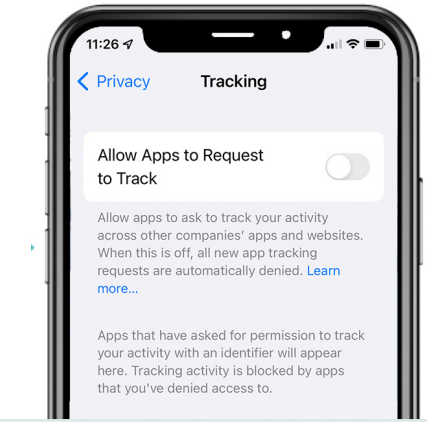
After all of the stressful hours and late nights preparing your app for Apple's AppTrackingTransparency framework, the last thing you want is to read another article about it, right? Yeah, we get that. But we uncovered some revealing information that shows your work isn't done quite yet.

At this point, most iOS consumers have installed and opened an iOS app and been prompted with the now-famous question about tracking. Apple requires consumers to opt-in to tracking, and if they don't, the app should not be collecting behavioral data and using it for advertising.

Ultimately, this makes it much more difficult to find and model audiences because the data simply isn't there. The shift to privacy-first app marketing techniques won't happen overnight but steps can be taken to minimize your exposure to data leaks and privacy breaches.

So first, to understand where the iOS ecosystem is at this moment, we did some in-depth research that takes a snapshot of the network connections iOS apps are still making when permission to track is not granted. The results may shock you and inspire your marketing team to take a closer look at the connections your app is making in the context of a first-party strategy.

We'll also share some steps you can take to help your marketing and app development teams get in sync and turn privacy into a competitive advantage.



Apple users must opt-in to app tracking

Why focus on iOS?

Apple is the current leader, steering the industry toward a more privacy-centric advertising model. But Google isn't far behind.

Google's privacy roadmap is centered around innovations that don't require users' personally identifiable information (PII), and we anticipate the release of an "app privacy" tool. Google has even gone so far as to promise new privacy innovations that will make third-party cookies obsolete.

This is a developing topic that will likely evolve as consumer awareness grows.

Taking the Covers Off Third-Party Tracking

In the release of iOS 15.2, Apple introduced customers to a new reporting tool called Record App Activity which we used to do this research. Any user can access this tool from their iPhones. Apps have always been a bit of a black box but this tool finally takes the covers off.

We analyzed 200 popular apps across 20 categories selecting a sample of about ten apps within each category. Each app was only downloaded and opened once without registering for the service to see and understand the app's starting set of connections.

Marketers beware, the app activity recorder gives consumers a window with a view into all the domain connections an app is making and instantly understands which connections are to a third-party or to an unidentified IP address, which is even more worrisome and suspicious.

Shockingly, even when permission to track is denied, we found there was still on average 15 potential tracking connections with ***80% to third-party domains.***

First-party connections imply that the company is using the data for their own marketing purposes and it's not being sold or shared for advertising. Third-party domain connections, on the other hand, typically lead consumers to an unknown domain or IP address.

Connecting to obscure third-party domains or unknown IP addresses will raise questions among consumers that there could be data sharing happening without the user's permission.

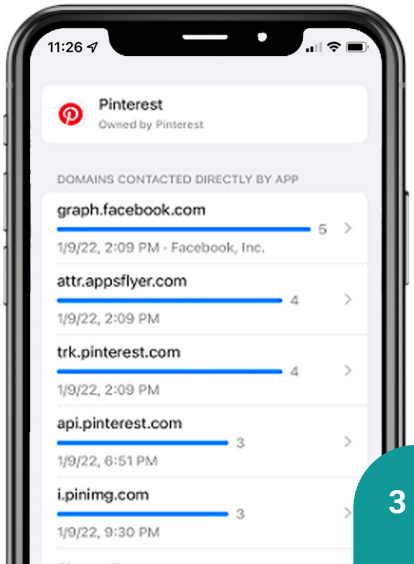
Looking at the big picture, we discovered between 4 and 28 connections are being made when permission to track is not granted. The results show that the industry still has a long way in the effort to build trust with consumers.

80%

of unpermitted tracking connections are to third-party domains

How to access iPhone privacy reports:

1. Go to settings > Privacy > App Privacy Report
2. Select an app under App Network Activity



Select Findings by App Category

The findings get even more interesting by category. Magazine apps had the highest number of total network contacts (28), and the highest percentage of third-party domain contacts (93%).

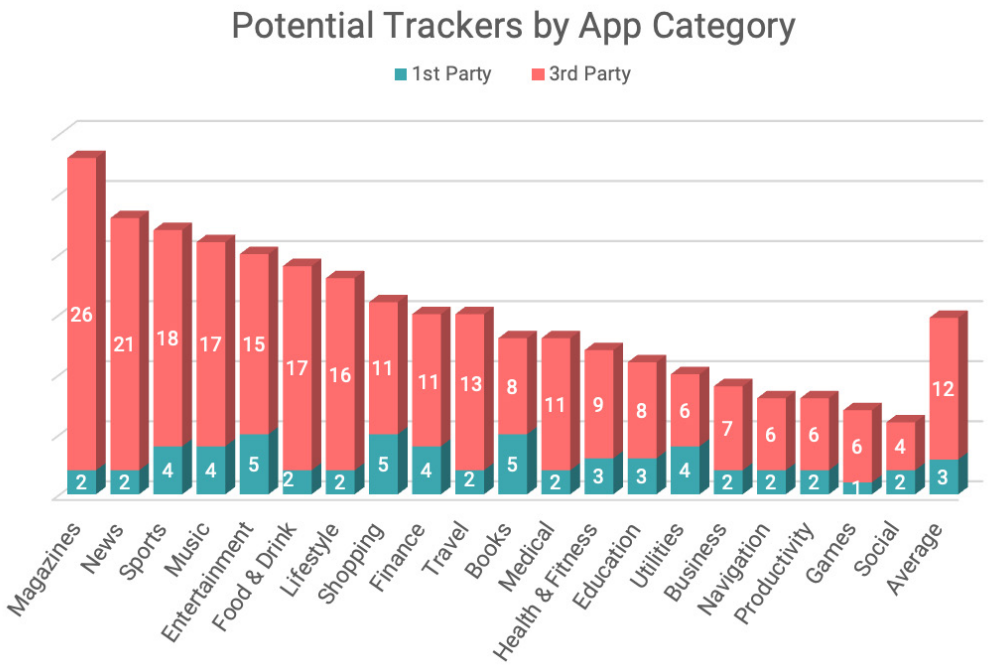
What do all of the categories with the highest number of potential trackers have in common? A business model that relies heavily on ad revenue. So, it may not be surprising to see them leading the connection count.

On the other side of the spectrum, we have categories like Utilities, Productivity, and Games, all with six connections each. That may not sound too bad compared to apps with well over 20 connections, but these connections are still established when someone opts out of tracking.

Every category, whether it's finance or fitness has what appears to be the worst and least tracking offender. Even one unexplained connection could cause concern among your customers and prospects.

We also noticed that some app connections are encoded as IP addresses, making them difficult to identify. Zoom did this for example, and it seemed like a red flag at first, but when we performed a reverse IP address lookup, we found that the domains were owned by Zoom and qualified as first-party data connections.

Brands will create a stronger trust impression if all of their first-party connections are easily identified or labeled as such. Some third parties may intentionally limit a users' ability to recognize who owns a domain. Marketers can challenge each connection's usefulness and request more transparency from third-party solution providers.



When we look across categories, it's easy to spot the worst offenders:

Magazines
26 connections

News
19 connections

Sports
18 connections

Music
18 connections

Entertainment
17 connections

Want more data?

Scan or click this code to view our full report.

Matching Perceptions with Reality

As consumers get savvy in using the app activity recorder, they are likely to view these connections as a betrayal of trust and delete certain apps.

For some apps, certain third-party connections may be needed for the app to function properly. What's interesting from our research, however, is that there can be a widely different number of third-party connections among apps in the same category, which inspires a lot of questions:

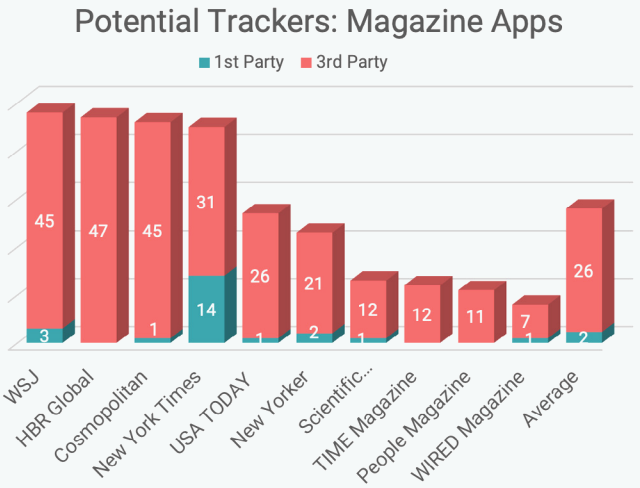
- **Is your app unintentionally sharing customer data which is then used for targeted advertising without the consumer's knowledge?**
- **Why do some apps in the same category make a lot more third party domain connections than others?**
- **How does your app compare to other apps in your category when it comes to third-party domain connections?**
- **When your customers look at your app's activity report, what do you want them to see and how are they perceiving it?**

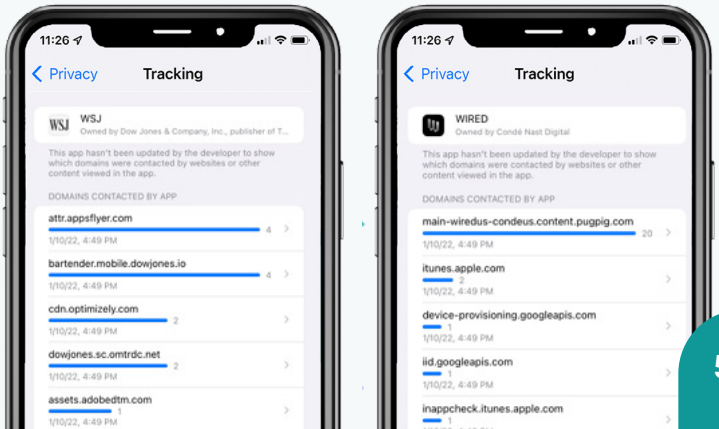
Magazines and Newspapers

We analyzed 10 apps in the Magazine category, including *HBR Global, Cosmopolitan, Time Magazine, The New York Times* and the *Wall Street Journal*

Key Findings

- **Average of 28 contacts**
- **93% of contacts were to 3rd party networks**
- **7% of contacts were to 1st party neworks**
- **WSJ made the most contacts (48) with 94% being 3rd party networks**





Food and Drink

We analyzed 10 apps in the Food and Drink category, including Popeyes, Publix, McDonald's, DoorDash, and Uber Eats

Key Findings

- **Average of 19 contacts**
- **92% of contacts were to 3rd party networks**
- **8% of contacts were to 1st party networks**
- **Popeyes made the highest number of connections (42), all to 3rd party networks**
- **Uber Eats made the fewest number of connections (4), 75% to 3rd party networks**

The answers to these questions over time will become more important as consumers get accustomed to using this tool to "track" potential tracking connections.

Prediction: Apple will introduce even more transparency features and requirements into their activity recorder such as displaying who owns the domain the app is connecting, what the connection does and exactly what data is collected and how it is used.

Apps with fewer third-party connections are better positioned in their efforts to build trust with consumers. Fewer third-party connections also points to a stronger first-party data strategy and business model compared to competitors in the same app category.

Is your brand's list of network connections causing undue alarm among your customers or is your app leaking valuable behavioral data? This is an area where your marketing and development teams can work together to make sure consumer perceptions match reality.

Prediction

Apple will introduce even more transparency features and requirements into their activity recorder such as displaying who owns the domain the app is connecting, what the connection does and exactly what data is collected and how it is used.

What It Means for App Marketing

Your brand's privacy reputation will increasingly be viewed as a competitive differentiator. In that context, your app's domain connections are an important signal that your company takes privacy seriously and you are in compliance with the latest privacy policies from Apple and Google.

Your brand's app could be at a competitive ***disadvantage*** if it's making a significantly higher number of third-party connections compared to other apps in the same category. Minimizing your app's network connections could prevent your brand from being called out in articles about surveillance marketing.

If your app already has fewer domain connections than other apps in your category, you could have a competitive ***advantage*** over other apps. Consumers using Apple's activity recorder will make judgments (true or not) about what their apps are doing with their data and why.

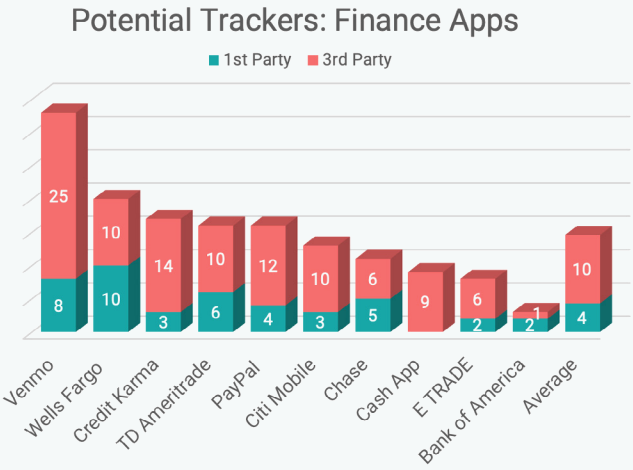
Brands should view the domain connections listed in the app activity recorder as an opportunity to build consumer trust when customers do not want to be tracked. You can also tie select benefits to certain types of tracking to inspire customers to opt-in.

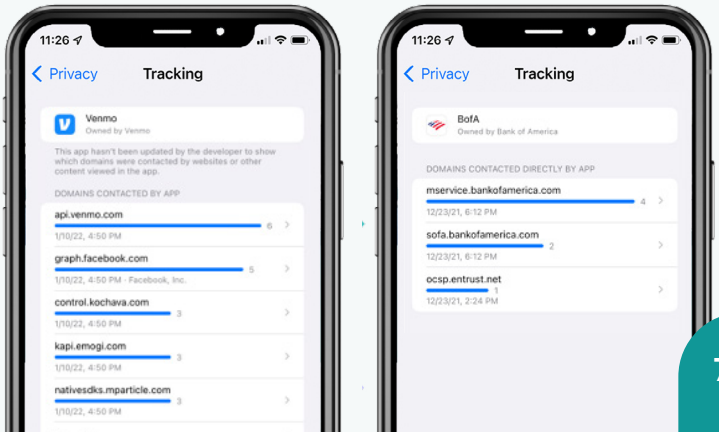
Finance

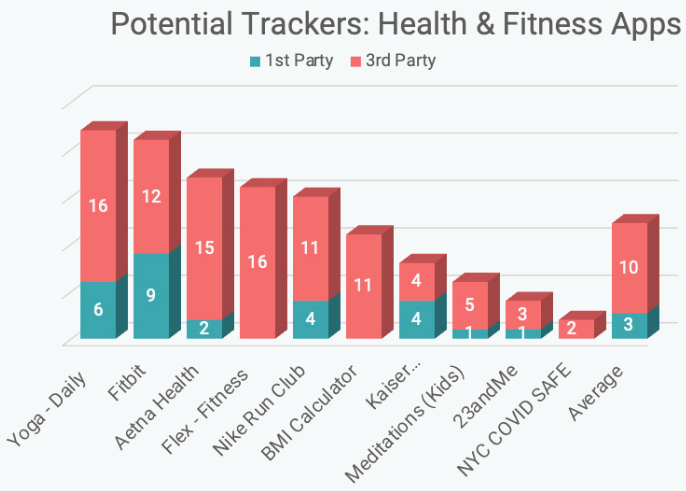
We analyzed 10 apps, including Citi Mobile, Wells Fargo, eTrade, Venmo and PayPal

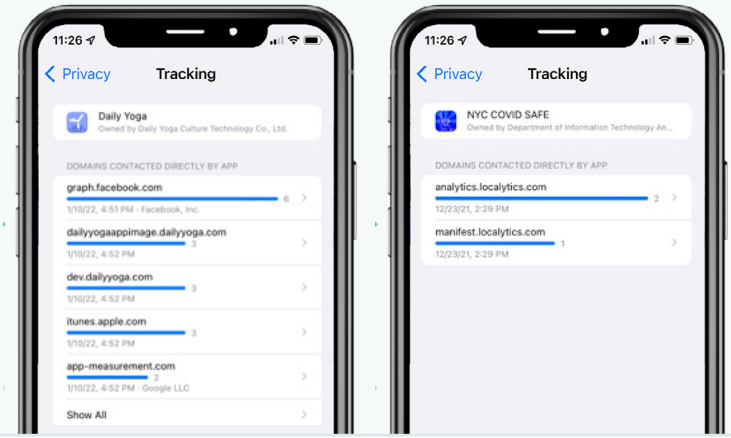
Key Findings

- **Average of 14 contacts**
- **69% of contacts were to 3rd party networks**
- **31% of contacts were to 1st party neworks**
- **Venmo made the highest number of connections (33) with 76% being 3rd party**
- **Bank of America made the fewest number of connections (3), with 33% being 3rd party**









Health and Fitness

We analyzed 10 apps in the Health & Fitness category, including Fitbit, Nike Run Club, Aetna Health, Kaiser Permanente, 23andme

Key Findings

- **Average of 13 contacts**
- **80% of contacts were to 3rd party networks**
- **20% of contacts were to 1st party neworks**
- **Yoga Daily made the most contacts (22), with 73% being 3rd party networks**

Keep in mind, Apple's transparency framework doesn't turn off connections for your customer if permission to track is not granted. A high number of third-party connections when customers opt-out of tracking creates the impression that their request was ignored.

If consumers discover your app is tracking — or even appears to be tracking, despite their request not to be — they won't blame third parties.

They'll blame you.

The domain connections an app is making is a reflection of the brand and perceived intentions when it comes to handling consumer data.

Yes, you've made a massive effort to comply with Apple's new privacy framework, but your work isn't done yet. Stay vigilant and monitor your app's domain connections to safeguard your brand's reputation. If your customers delete your app

> ***If consumers discover your app is tracking despite their request not to be — they won't blame third parties. They'll blame you.***

because of privacy concerns, you've lost control of the conversation, not to mention valuable engagement signals and even revenue.

Advertisers, however, do need tools to measure engagement and grow their install base, and third-party solutions are viable options. The new requirement, however, is privacy. Network connection transparency puts pressure on developers and marketers to shift their strategies toward the use of privacy-first solutions that help increase engagement in ways that strengthen first-party data without compromising your app's data.

Are your development and marketing teams fully in sync on privacy-first data strategies? Probably not and at first glance, your marketing team may not even have a clear understanding of what these connections are doing or how the number of connections your app is making compares to other apps in your category. But now you have a starting point.

Challenge your team by asking if the domain connections your app is making are truly needed. You may find they can be replaced with more modern privacy-first technologies.

How to Minimize Third-Party Domain Connections

The first step is to understand the list of domain connections your app is making. Discuss with your team how to communicate to customers what each connection is doing, the data collected and how that data is being used, stored and shared.

The next step is to limit the number of software development kits (SDKs) your app uses. SDKs increase your exposure to third-party connections and may even introduce new connections without your marketing team's permission or knowledge.

Perform an audit of your app to assess your technology stack. Once you have a clear view of what data is shared with third parties, start asking questions:

- ***What connections are my SDKs making?***
- ***Are these connections reflecting poorly on my brand?***
- ***Can these SDKs and connections be replaced with privacy-first, codeless solutions?***
- ***Are third-party companies using my app's data to create device-level profiles which circumvents Apple's privacy policies?***
- ***Is my app's data being shared with data brokers?***

App Audit Notes

Moving Forward

The future holds a more secure, privacy-first environment where customers have more control over their data. In the meantime, is Apple enforcing its own policies? Maybe not, perhaps that's why the app activity recorder was released—so users can do the policing.

The compliance burden falls not only on Apple but all parties. Apple, app owners and consumers will continue to be active participants in the privacy conversation and the effort to move the industry forward. We anticipate a growing demand for in-app privacy controls and app owners to incorporate them into their development strategies.

The bad actors in the app ecosystem, however, are likely to double down on their elusive tactics. Companies that need device-level data will find ways to use a brand's domain, implying first-party data collection and use. Other connections still opt for ambiguity by listing only an obscure domain, preventing consumers from easily understanding how their data is used.

Similarly, we expect more connections to rely on numerical IP addresses instead of domain names. To combat this, Apple's App Privacy report will probably begin showing who owns the domains an app is linking to, similar to how the report currently indicates that app-measurement.com is owned by Google.

As transparency and privacy controls become more robust, brands will move their marketing efforts away from third-party surveillance tactics, choosing instead solutions that strengthen first-party data and their relationships with customers and prospects.

Brands that get their first will be best positioned to win the hearts—and the wallets–of consumers.

Request your free App Transparency Audit

Scan the code or email us to get started

URL GENIUS

info@urlgeni.us

urlgeni.us

@urlgenius

/urlgenius

About URLgenius

URLgenius is the leading provider of SDK-free app linking and QR app marketing experiences. Trusted by leading luxury, financial, and consumer brands around the world, URLgenius can help you create seamless app experiences that optimize conversion, engagement, and revenue, without compromising PII data.

Appendix: How we did our research

We used the Record App Activity feature introduced in iOS 15.2 and ran an App Privacy Report to compile the data. Each app was downloaded and opened only once. After opening, “Allow Apps to Request to Track” was disallowed. Then we took a screenshot of the trackers that were subsequently still installed.

Although some domains contacted by an app may be required for certain functionalities, those connections were still counted in the tally because of their potential for other actions, like sending behavioral app data to an analytics service or ad networks.

Our research only included iOS devices because this type of insight isn’t available through Android — though Google’s privacy roadmap suggests it’s not far off.

URL GENIUS