REPORT

Who's Stalking Mobile App Users?

Finding and controlling the third-party code (3PC) app publishers don't know about

THE MEDIA TRUST

We know digital security.

Executive Summary

Whose eyes are watching mobile app users? Today's device-toting consumers spend 90% of their time online on mobile apps[1]. Yet they have little to no notion they're under the watchful eyes of a broad range of companies—many they've never even heard of—that form these apps' digital supply chain. Unfortunately, the app publishers are too often only slightly more aware of the companies that stalk their users.

This report takes a unique look at the largely unknown, uncontrolled third-party code (3PC)[2] that enables the functionality of 10 of today's most popular mobile apps on the Apple store. It also explores this code's impact on users and mobile app publishers, with an eye to dispelling the misguided notion that since "cookies do not work on mobile" little data being harvested. The aim of this research is to provide top management teams and boards with information they can use to avoid the costly fines and brand damage that can result from the misuse or theft of user data.

In August 2019, The Media Trust monitored 10 of the Apple App Store's most popular "Shopping" (Shop) and "Food & Drink" (F&D) mobile apps in order to uncover[3]:

- Which digital vendors leverage code to access users' information
- What information is being tracked or collected on users as they install the app and as they make purchases
- The regulatory risks third- and nth-parties pose in gathering users' information, in particular the data leakage/breach risks these vendors introduce to popular apps and their users
- The regulatory risks that mobile app publishers shoulder by allowing unseen code from largely unknown vendors to run on their digital assets

90%

of mobile app calls are made to third parties

[1] https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

[2] Code run by digital vendors

[3] Apps have been anonymized under the principle of responsible disclosure in order to give app publishers the opportunity address the security and privacy issues that The Media Trust uncovered.

Key Findings

90%

Percentage of all calls, on average, that are made to third parties

13

Average number of vendors during install:

23

Average number of vendors during purchase

1.5 years

Average cookie lifespan:

67%

Percentage of cookies that are persistent

- Third parties most frequently seen across mobile apps are large technology companies that manufacture devices or provide digital services such as social logins, cloud infrastructure, or analytics.
- Third parties increase the security and privacy risk, as each one expands the number of infiltration vectors.
- Compared to F&D apps, Shop apps drop more third-party cookies, have more third-party domains present in the install and purchase phases, and drop far more persistent cookies (ie, whose lifespans exceed session).
- Shop apps run a greater risk of noncompliance with data regulations, such as GDPR and CCPA.

Introduction

Mobile apps offer consumers convenience and speed. These apps let them obtain products and services anywhere consumers have access to the internet. With apps, consumers can purchase shoes, household goods, meals, etc. That convenience, however, comes at a price that increasingly wary consumers are aware of—their privacy. App developers like to collect user data to improve the user experience; malware and spyware developers do the same to steal or commit fraud.

The shift in consumers' awareness is taking place as a result of data privacy regulations like GDPR and CCPA and the growing number of high-profile data breaches and abuses. The upshot: companies that have any digital presence must do a better job of knowing what user information is collected and processed, for what purpose, and by whom each time users install apps and make purchases.

There are key challenges to reducing the risk of unknown code running on apps:

- Most apps are not designed with security and privacy in mind.
- Third parties and their suppliers can—and do—change between the install and purchase, sometimes doubling the number of third- and nth-parties that can access user information.
- Bad actors know that third parties and their unmanaged code make for soft targets.

Add to this data privacy laws that are being introduced around the world, giving regulators authority to hand down unprecedented penalties.

Our aim with this research is to offer top management teams insights into the hidden vulnerabilities of their mobile apps, as well as suggest ways to fortify their defenses and drive down their digital risks.

Research Results

DIGITAL VENDORS DOMINATE

A total of 351 distinct domains appeared in the entire group of 10 apps across both phases. The distribution is positively skewed as the average of 35.1 exceeds the median of 31. Shop 1, Shop 3, and Shop 4 accounted for 49% of the total count.

351 distinct third-party domains in the mobile apps

The vast majority of these domains were supplied by third parties (Figure 1), accounting for an average of 90% of all executing domains. This is a stunning percentage of code that lies outside app publishers' control. Without the right people, process, and tools, publishers would have no idea who the code was coming from, what it was doing, or why it was there.

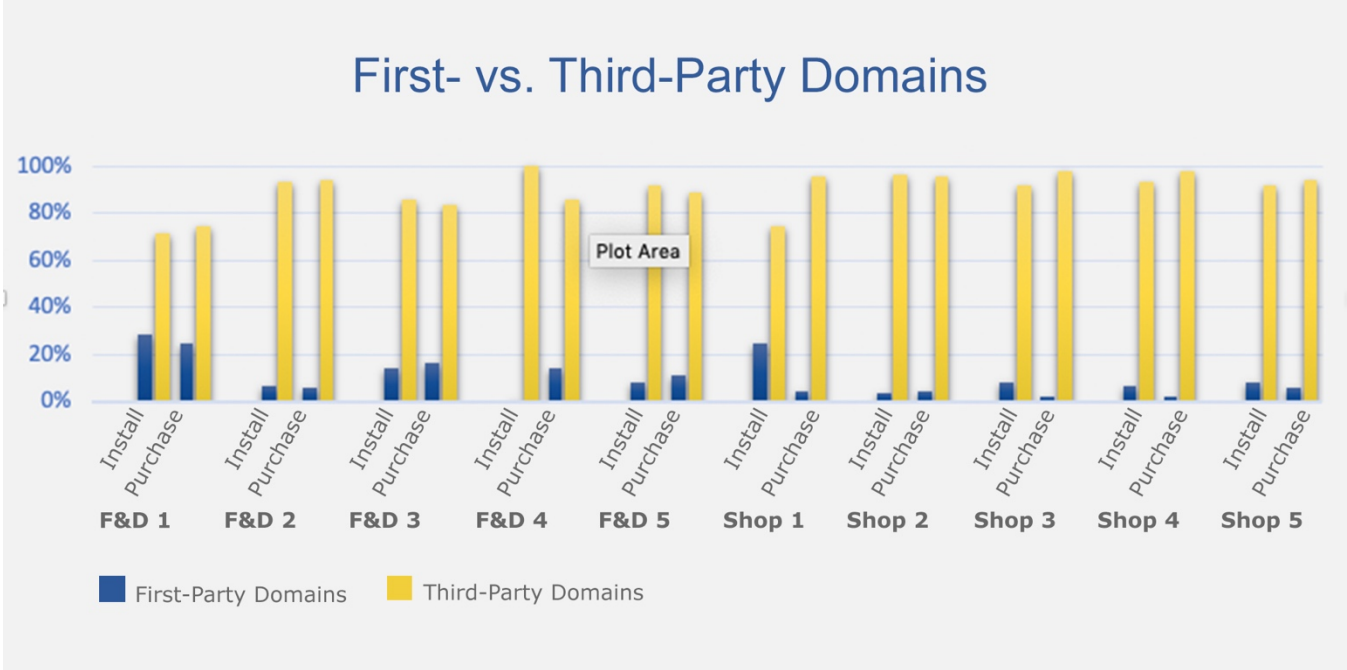

Figure 1: Third-party domain calls across mobile apps

The potential for unauthorized third and nth parties' access to user information presents regulatory headaches. Data privacy regulations often require companies to enforce the restrictions throughout their network of third parties through contracts and compliance monitoring. Without an accurate view of third-party code, publishers have no way of maintaining compliance but would be liable for their third party's violations. GDPR and the upcoming CCPA both require companies to ensure their third parties' compliance.

The top 5 domains and sources of cookies found across many of the apps belong to the following companies[4]:

1. Big
2. Treez
3. Eev
4. Klay
5. Album

These companies dominated the install and purchase phases. Their dominance likely has to do with providing any of the following:

- Cloud infrastructure
- Mobile devices
- Social login
- User analytics for publishers

LAUNCH VS. PURCHASE

Domains

A closer look at the data shows that the number of domains change from launch/install phase to purchase phase (Figure 2). In seven of the apps—F&D 1, F&D 2, F&D 4, Shop 1, Shop 3, Shop 4, and Shop 5—the domain count rose during purchase. In fact, for Shop 1, Shop 3, Shop 4, the number of domains spiked to more than twice the number during install. For the rest of the apps, domains slightly dipped during the purchase transaction.

[4] Listed using pseudonyms under the principle of responsible disclosure in order to give the app owners involved the opportunity to address the privacy issues with the domain owners.

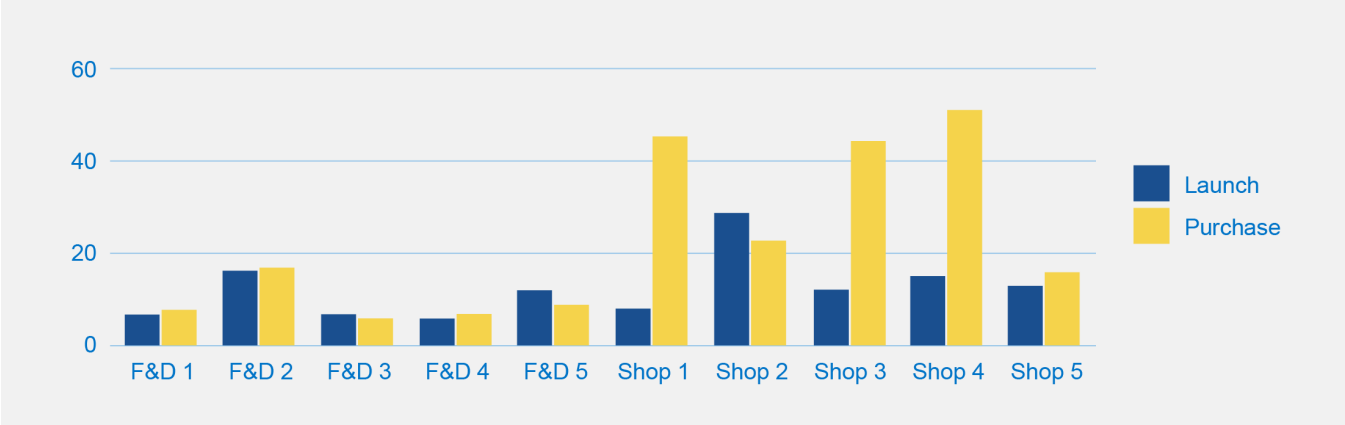

Figure 2: Domains by phase

Cookies

A total of 142 cookies were dropped across nine of the 10 apps (Figure 3). Shop 4's cookies alone accounted for 23% of overall cookie count. Add to this Shop 3's and Shop 1's cookie counts, the total equals a whopping 67% of all cookies dropped. Moreover, the number of cookies these apps dropped between install and purchase soared by a factor of three. Meanwhile, F&D 4 and F&D 5 dropped zero cookies.

142 cookies dropped across 9 of the 10 apps.

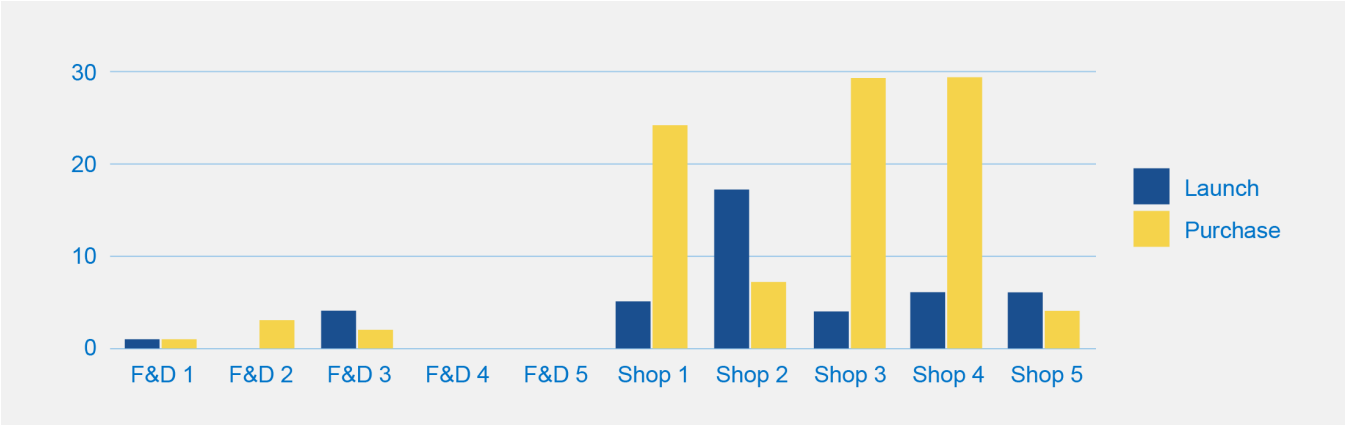

Figure 3: Cookies by phase

These two extremes, where three Shop apps dominate the cookie count while two F&D apps drop no cookies at all, illustrate the marked contrast between the two groups of apps. The former drop far more cookies than the latter. One likely explanation for this difference is that Shop apps offer more features, such as ads on brands the retailers carry, image libraries, videos, etc., to drive the purchase. F&D apps have less need for ads. Restaurant apps, in

particular, feature their own products only. Food and drink delivery apps that serve as marketplaces do not serve ads on restaurants they serve.

Another marked distinction has to do with the ratio of first- to third-party cookies. F&D apps drop few, if any, third party cookies (Figure 4 and Figure 5). Furthermore, Shop cookies tend to be more numerous during purchase.

Figure 4: F&D cookies during install and purchase

Figure 5: Shopping cookies during install and purchase

Users enter names, email addresses, and other personal information to install and submit payment information to make purchase transactions. Most users think only app publishers can

view all this information. Although app privacy policies often mention what information is processed and by whom, users readily agree with these policies without paying attention to the details. As a result, most users—and the publishers themselves—remain unaware that third parties have access to their personal information. It's important to note that each vendor represents an attack surface or hacking target. As more third-party domains appear during the purchase phase, user information—in particular payment information—becomes more vulnerable to theft and abuse by hackers and unscrupulous vendors.

Close to half (49%) of the domains that drop cookies are known advertisers, 21% are ad servers or networks, and 18% are targeting or statistics companies that provide publishers with app performance analytics (Figure 6). While advertisers and ad servers/networks use these cookies for targeting, following users around the internet in order to build up these users' profiles, app analytics companies help publishers better understand their users. For this reason, some researchers classify performance analytics cookies as first-party cookies.

The Media Trust considers all cookies and domains that do not fall directly under the app publisher or under the publisher's parent or sister company as those under the control of third parties. The underlying assumption is that monitoring cookies from parent- or sister-companies for compliance or digital policy enforcement is easier than those from third parties. Enforcement becomes even more challenging when third parties fail to disclose who they are (those labeled "TBD/Needs more data") or have been involved directly or indirectly with past malicious campaigns (those labeled "Suspicious"). While these two groups constitute only 5% of domains, they can expose app publishers and users to significant security and privacy risks. One such third party has been known to auto-redirect users to app stores.

Advertiser	49.3%
Ad Server / Network / Optimizer	21.13%
Targeting / Stats / Privacy	17.61%
Publisher	5.63%
Suspicious	2.11%
CDN / ISP / Hosting	2.11%
TBD / Need more data	2.11%

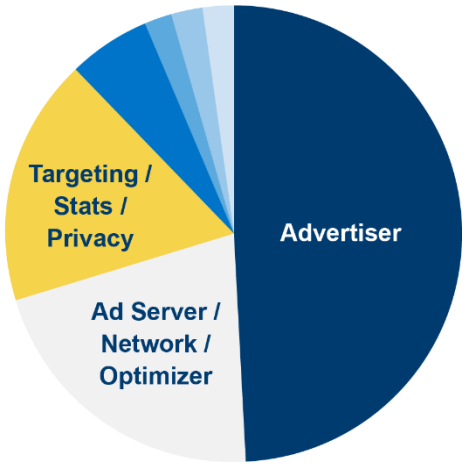

Figure 6: Domains that drop cookies

In fact, data privacy regulators focus not only on who collects what information, but also how long cookies stick around after the browser session has ended. Close to 67% of all cookies dropped persist beyond the browser session. These cookies last anywhere from one day to more than 5 years. The cookies in this research had an average lifespan of 1.14 years. One of the cookies had a lifespan of 20 years.

67% of cookies had lifespans that exceeded the browser session, a violation of GDPR and the French cookie law.

Cookie lifespans are another area of difference between the two app groups. Session cookies account for 44% in the F&D group but only 30% in the Shop group. Close to 7% of Shop cookies last longer than 3 years. F&D cookies don't exceed five years.

0 -1 Year	44.44%
Session	44.44%
1 - 3 Years	11.11%

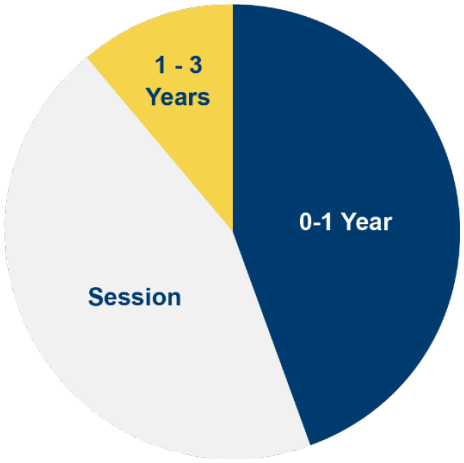

Figure 7: F&D Cookie Lifespan

0 - 1 Year	41.1%
Session	30.14%
1 - 3 Years	20.55%
5+ Years	6.85%
3 - 5 Years	1.37%

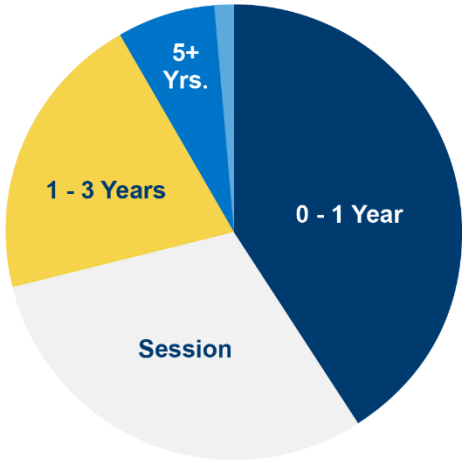

Figure 8: Shop Cookie Lifespan

Originally designed to help publishers track user behavior in order to improve user experience, cookies have become notorious for being invasive. For this reason, the EU's ePrivacy directive limits the duration of active cookies to 12 months. France's data protection authority (CNIL) limits cookie lifespan to 13 months. The study indicates that the Shop apps face greater risk of violating data compliance regulations.

Questions & Answers

QUESTIONS MOBILE APP PUBLISHERS SHOULD KNOW THE ANSWERS TO

Apps are magnets for bad actors who want to spy on and steal from consumers who spend up to 90% of their time online using apps.[5] Our work with mobile app publishers indicates that many do not have the teams, tools, or the time to closely monitor the actors and activities in their digital ecosystem. In fact, without these resources, app publishers remain unaware of their ecosystem's complexity—that there are numerous unknown vendors in their midst; dynamism—that these players can switch by the session and by the user; and opacity—that unless they know what's showing up on users' devices, they can't confirm which code is doing what. If most security—or privacy—teams are not acquainted with their authorized suppliers, how would they know if unauthorized parties have infiltrated the ecosystem?

> While cookies in a mobile app are sandboxed from those in another, they still harvest user information… How it's used and whom it's shared with is anyone's guess.

What they don't know *will* hurt them. Digital threats are on the rise and, as data privacy laws spread across the world, so is regulatory risk. This study shows that the 90% of calls that are made while users install and make purchases on apps go to third parties, who can access user information through cookies and other means.

These risks cannot be addressed solely by the security team. In most cases, a variety of stakeholders are responsible for the business's digital assets, the first and most important touchpoint for a business's market. The problem is, despite digital assets' pivotal roles to the business, too often security teams, already saddled with tasks they don't have enough resources take on, are left holding the bag. Yet, the individuals that inked contracts with the vendors supporting these assets likely belong to marketing or other teams.

[5] https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

To address the risks that come with digital assets, security and privacy teams must work together on findings answers to the following key questions:

1 What code is running on my app and who's supplying it?

Without the right resources, there is no way to know. App publishers should work with experts on monitoring their apps for unauthorized actors and activities. Much of the calls (90%) in an app lie outside the publisher's control and are made to third parties, who have their own network of contractors. These third parties collect user information in real-time, ranging from data users enter to screenshots. Policing these third and nth parties' activities is both time- and resource-intensive because of the digital supply chain's lack of transparency, dynamism, and complexity.

2 Why should I be concerned about privacy when cookies aren't able to track my behavior from app to app?

There is much confusion over the role cookies play in mobile devices. While it is true that cookies in apps are sandboxed from each other and, therefore, fail to provide marketers the ability to track users across apps, these cookies still harvest user information and they are not the only means for apps to siphon user identifiers. If you regularly use your favorite clothing retailer's app to shop, you probably don't want to keep entering your credentials or credit card information each time. Your app's third-party code collects that and other personally identifiable information through various methods so you don't have to keep entering it. Some apps have been found to collect Advertising IDs in addition to persistent identifiers like device IDs.[6] Once that information has been collected, how it's used and whom it's shared with is largely unknown.

[6] https://nakedsecurity.sophos.com/2019/02/19/thousands-of-android-apps-bypass-advertising-id-to-track-users/

3 Are my digital vendors' code in line with my policies?

Knowing who's in the digital ecosystem makes it easier to share and enforce digital policies. Many vendors carry out crucial activities to help publishers meet their users' demand for ever richer experiences. They gather behavioral and other data for legitimate purposes. However, regardless of purpose, data collection might not always align with some publishers' policies. If laws like CCPA and GDPR hold publishers to account for their vendors' actions and security measures, publishers must continually monitor for any policy violations and root out repeat offenders. Or, they risk footing the bill and being blamed for noncompliance.

4 Is my users' information safe?

Data privacy laws like GDPR and CCPA require businesses to provide adequate security protections to their users' information. This means carefully vetting digital vendors for security, avoiding those who have weak security measures, and assuring activities don't put users' information at risk. Vendors tend to be popular targets among bad actors who know too well that many vendors give little importance to security and privacy yet offer access to thousands if not millions of app users.

Conclusion: Protecting Top and Bottom Lines

Apps are critical to a growing number of businesses. Along with websites, they help businesses attract and engage prospects and customers. While these web assets play mission critical roles, they are subject to a growing number of data privacy laws that hand down stiff penalties to companies in violation. Such violations often grab headlines and can erode a company's reputation with consumers who have grown weary of data breaches and abuses. Today, consumers will not entrust their business to companies that can't be trusted with their

information. Knowing the answers to these questions will help app publishers to protect their users from malicious actors, comply with existing data privacy laws like GDPR and kick start a program for CCPA compliance, and, in so doing, protect their top and bottom lines. Unless publishers can monitor the activities of third-party code from users' side, these digital strangers will hurt users and, as a result, their business.

Appendix: Research Methodology and Analysis

The Media Trust carried out in-app client-side scans of 10 of the Apple store's most popular apps. Five were among the top 50 in the "Shopping" category and the other five among the top 50 in the F&D category. Each had more than 5M installs and were rated at least 4.6 out of 5 stars.

The Media Trust conducted client-side scans throughout two phases: (1) install and configuration and (2) purchase transactions. The scans captured how many and which vendors were present, the number of cookies dropped, and the lifespan of cookies dropped.

The research focuses on iPhones to explore ways users can be exposed to security and privacy threats even when using devices designed with privacy and security in mind.