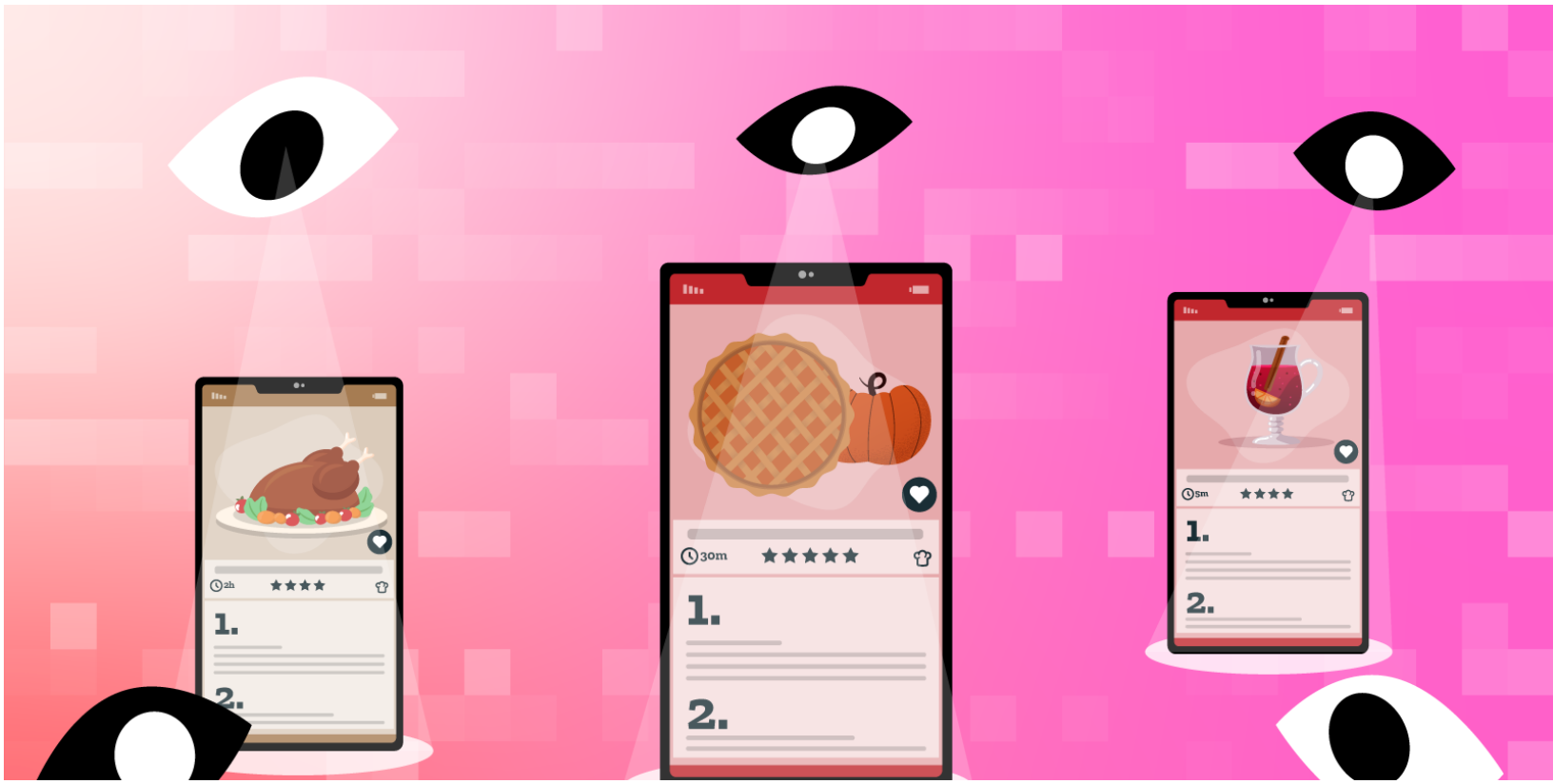


Uninvited guests: Popular Android recipe apps are loaded with trackers

Mozilla Foundation | November 2021

Author: Becca Ricks

moz://a

Table of Contents

Introduction & Summary

Ad tracking across apps has become increasingly sophisticated over the past decade. Major advances in personalization occurred with the introduction of Apple's Identifier for Advertisers (IDFA) in 2012 and Google's Android Advertising Identifier (AAID) in 2014. Both IDs are random device identifiers assigned to the user's device that are constantly being transmitted in app traffic. These identifiers help advertisers more easily identify, track, and target individuals across various apps and services.

In June 2021, Google announced that in 2022 it will update ad tracking on Android so that users have the option to opt out of Android ad ID tracking. This announcement came after Apple implemented sweeping changes to app tracking on the iPhone, so that users have to *opt into* any tracking at the point of use.

On their face, these announcements are huge steps forward for privacy – as long as they are actually enforced. (A big if for Apple, which is struggling to enforce its new rules for ad tracking). Meanwhile, third party tracking is still the default on Android. **This means that unsuspecting Android users will continue sharing their data without realizing it.**

Given this landscape, Mozilla aimed to get a snapshot of how Android apps are currently sharing personal data. Ahead of Thanksgiving 2021, we analyzed the network traffic of 8 cooking apps to determine what pieces of user data are being transmitted to third parties.

In our investigation, we found that:

- All of the apps were sharing data with advertising/marketing companies. **The most data-hungry apps were Recipes Home, Allrecipes, and Food Network Kitchen.**
- The most common third party ad trackers were Facebook and Google DoubleClick. The ad trackers MoPub, Branch, Kochava, Tapjoy, and Vungle in particular collected a lot of device data. The most common analytics trackers were AppsFlyer, Apptentive, Google Analytics, and Adjust. *(Full disclosure: Mozilla Corporation products use Adjust for analytics and advertising conversation measurement).*
- **At least 6 of the apps were sharing ad IDs with advertising/marketing companies.** In many cases, this included: advertising IDs, precise location data (latitude/longitude), and device data (model, make, OS version, etc). A number also were sharing behavioral data – app clicks, scrolls, and views – with advertisers.

Methodology

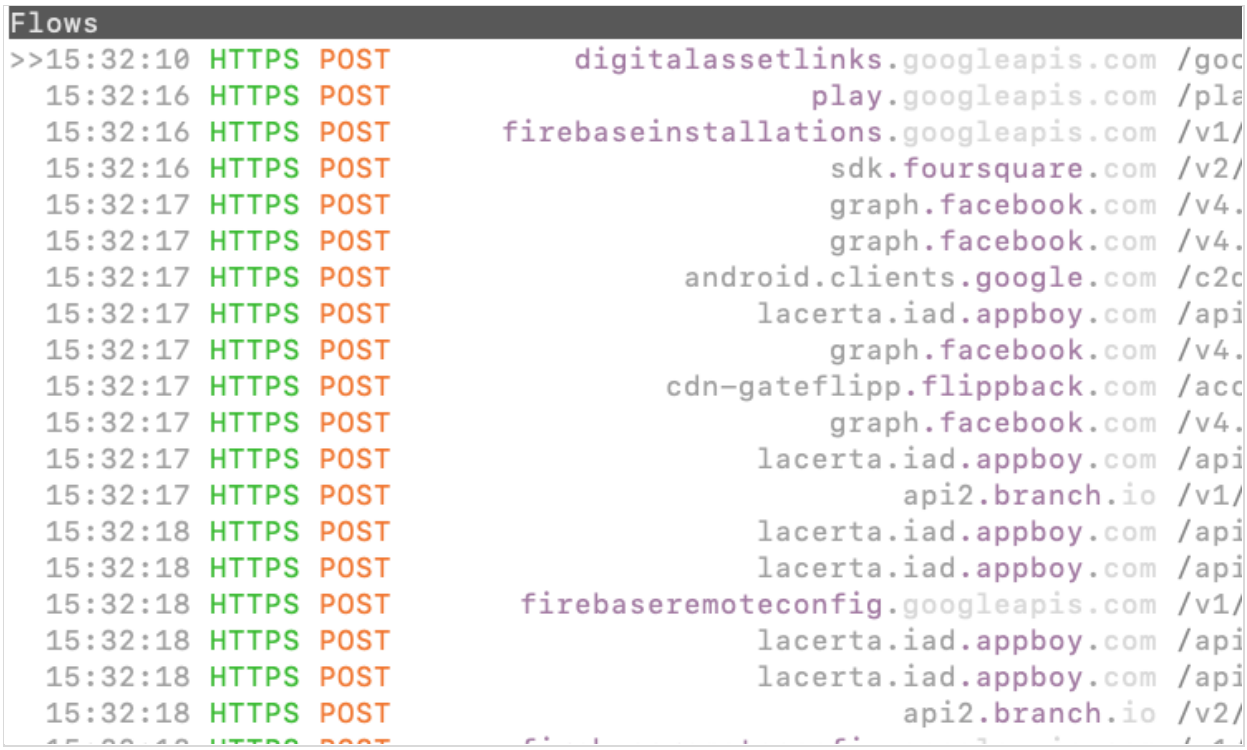
The goal of this project was to better understand how Android apps are currently collecting people's data. We aimed to learn who the most active third party trackers are and what user data they are collecting.

With Thanksgiving and the holiday season approaching, we decided to focus our attention on cooking and recipe apps. We started by looking at the 18 most popular free cooking apps in the Food & Drink category in Google Play Store that were also compatible with our tester mobile device. After observing how those apps shared data, we narrowed down our analysis to 8 apps: Allrecipes, Food Network Kitchen, BBC Good Food, Recipes Home, Whisk, KptnCook, Crockpot Recipes, and Flipp.

Using a Samsung device that had undergone a factory reset and a new Google account created just for testing, I systematically installed each app, scrolled through the app for 2-3 minutes with pauses, observed which third party trackers requested data from the phone, and then uninstalled the app.

To observe the app data flowing in and out of the phone, I used an open source tool called mitmproxy. Mitmproxy is a man-in-the-middle proxy with a command-line interface. It is used by developers to debug apps, but it's also used by privacy researchers to decrypt and view HTTPS web traffic. After installing mitm software on my computer, installing the root certificate on the device, and running the proxy on the host, I was able to intercept and decrypt the data flowing in and out of my Android phone.

Command to run mitmproxy in the terminal, filtering for POST requests.



A snapshot of how the traffic logs appear in the terminal: Time of request (15:32:10), type of request (HTTPS POST), server requesting data (facebook, appboy, branch).

Specifically I looked at HTTPS POST requests. A GET request is what your phone is asking for from a server; a POST request is what a server is asking for from your phone. I used mitmdump to capture the POST requests – the data that trackers were requesting from my phone – and then looked at what data they asked for. For instance, below you can see examples of two different requests, one from Facebook Graph and the other from Branch.

```JSON
{
    "advertising_ids": {
        "aaid":
    },
    "app_version":
    "branch_key":
    "brand": "samsung",
    "build":
    "connection_type": "wifi",
    "country": "US",
    "cpu_type":
    "debug": false,
    "device_carrier": "Searching for Service",
    "environment": "FULL_APP",
    "facebook_app_link_checked": false,
    "first_install_time":
    "google_advertising_id":
    "hardware_id":
    "install_begin_ts":
    "instrumentation": {
        "v1/install-qwt": "0"
    },
    "is_hardware_id_real": true,
```


Inspecting a request from Branch (redacted). Examples of user data collected: Android Advertising ID, Google Advertising ID, data about the device.

Detailed Research Findings

All of the cooking apps I analyzed had third party trackers, most of which were collecting user data for the purpose of improving advertising or marketing. Several of those trackers – most notably Braze, Branch, MoPub, Kochava, Tapjoy, and Vungle – collected a great deal of user data.

Summary of active trackers observed

App	Active Trackers Observed
Allrecipes Dinner Spinner	Amazon Ads Google DoubleClick Branch Facebook Graph Yahoo Apptentive

	Segment Google Analytics
Food Network Kitchen	BlueShift Facebook Graph Kochava Adobe Marketing Cloud Apptentive New Relic
BBC Good Food	Permutive SkimLinks Google DoubleClick Urban Airship Google Analytics
Recipes Home	MoPub Tapjoy Facebook Graph Unity3D Google DoubleClick Yahoo Nexage Vungle Adjust Google Analytics
Whisk	Braze Facebook Graph Google DoubleClick MixPanel Google Analytics
KptnCook	Iterable Branch Facebook Graph Revenuecat AppsFlyer MixPanel
Crockpot Recipes	MoPub Google DoubleClick Google Analytics
Flipp - Weekly Shopping	Braze Facebook Graph Branch

	Foursquare Google Analytics

These are the third party trackers we observed while running each app, but note that there are likely more trackers permitted by the apps to collect user data.

In the following sections, we'll go into further detail about what we observed. For each app, you'll see a table summarizing what user data was being requested and collected by third party trackers. Note that these are the pieces of data we observed being requested by trackers during our session, but trackers may be collecting even more data.

A couple of notes:

- The number under "Requests" was the number of times we received an HTTPS POST request from the tracker.
- In all cases, the user's IP address was shared with the tracker because it's required for connecting to a server.
- An N/A response under "Data requested" indicates that we were unable to parse the HTTPS POST request, either because we were unable to decrypt the data or because the data wasn't in a form we could analyze.

Allrecipes Dinner Spinner

Allrecipes Dinner Spinner is owned by Meredith Corporation, a media and marketing services company that owns PEOPLE, Entertainment Weekly, Real Simple, dozens of TV stations, and several targeted marketing companies. According to Meredith Corporation's privacy policy, the app collects data from your device via cookies, such as device information, IP address, and how you interact with the app. It may share data with advertisers, third party service providers like analytics firms, and other brands within Meredith.

In my observation of the data flowing out of the Allrecipes app, I saw a number of third party trackers requesting user data. Most of those third parties were advertisers collecting identifiers including Android Ad ID and device fingerprint ID, as well as detailed location data like latitude and longitude. Many also collected behavioral data – a record of your every activity on the app. Amazon Ads was the most active of these trackers, asking for user data 36 times in just two minutes.

Summary of user data collected

Tracker	Requests	Type	Data requested
Amazon Ads	36	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, orientation, language, connection type) - Ad identifiers (IDFA, Android Ad ID)
Google DoubleClick	23	Advertising	
Branch	13	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, orientation, language, connection type) - Ad identifiers (IDFA, Android Ad ID, Android ID, advertising IDs, Google Advertising ID, identity ID, device fingerprint ID, hardware ID) - Location data (latitude/longitude, locale)
Facebook Graph	4	Advertising	- Device data (model, make, OS version, country, carrier, time zone)
Yahoo	1	Advertising	*N/A*
Apptentive	13	Analytics	- Device data - Ad identifiers (advertiser ID, UUID) - Behavioral data
Segment	9	Analytics	- Device data - Ad identifiers (advertiser ID, device ID) - Behavioral data
Google Analytics	6	Analytics	*N/A*

Food Network Kitchen

The Food Network Kitchen app is part of a family of apps and websites owned by the Discovery corporation. In the app's tracking technology notice, it says the app may track device identifiers, advertising identifiers, cross device behavior, and precise location

information. Third party advertisers may use tracking technologies in the app to collect interaction data and serve up interest-based ads.

In my observation of app traffic, I saw a number of advertisers collecting identifiers including Android Ad ID as well as advertiser-specific IDs like Adobe's Experience Cloud Visitor ID, BlueShift's ad ID, and Kochava's app ID. In many cases, marketers combine several different identifiers together to identify the user and track them across devices, apps, and services.

Summary of user data collected

Tracker	Requests	Type	Data requested
BlueShift	5	Advertising	- Device data (model, make, OS version, country, carrier, time zone) - Ad identifiers (Advertising ID, customer ID)
Facebook Graph	3	Advertising	- Device data (model, make, OS version, country, carrier, time zone) - Location data
Kochava	3	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, screen brightness, volume, orientation, language, connection type, battery level, battery status, MAC address of client) - Ad identifiers (Android Ad ID, Android ID, Marketing Cloud Visitor ID, Kochava app ID, Kochava device ID, Network Transaction ID) - Location data
Google DoubleClick	2	Advertising	*N/A*
Adobe Experience Cloud	4	Advertising/ Analytics	- Device data (region ID) - Ad identifiers (Marketing Cloud Visitor ID, Customer ID, TNT ID) - Location data
Apptentive	9	Analytics	- Device data - Ad identifiers (advertiser ID, UUID) - Behavioral data
New Relic	8	Analytics	- Device data (model, make, OS version, country, carrier, time zone)

			- Behavioral data

BBC Good Food

BBC Good Food is an app run by BBC, which is owned by Immediate Media Company. The company's privacy policy explains that the mobile app has cookies that "help to make…ads relevant and interesting to you." Third party advertisers serve ads through the Immediate website and apps, including Google Double Click and "other vendors who have signed up to the IAB Transparency and Consent Framework," a Europe-wide framework for getting user consent for targeting with behavioral ads that has been challenged several times for failing to comply with GDPR.

In my analysis of the app, I noticed several advertising trackers, including Permutive and SkimLinks. Interestingly, Permutive uses IBM Watson to assign cohort categories to users – when I downloaded the app, my device told Permutive that I had been assigned the labels of "food and drink" and "technology and computing/internet technology/email." Compared to other food apps, though, these trackers didn't seem to collect much personal data.

Summary of user data collected

Tracker	Requests	Type	Data requested
Permutive	37	Advertising	- Ad identifiers (user ID) - Inferred data (IBM Watson cohort categories assigned, e.g. "food and drink", "technology and computing/internet technology/email")
SkimLinks	2	Advertising	- Device data - Ad identifiers (globally unique identifier) - Location data (country, state)
Google DoubleClick	2	Advertising	*N/A*
Urban Airship	13	Analytics	*N/A*
Google Analytics	9	Analytics	*N/A*

Recipes Home

The app Recipes Home - Easy Recipes and Shopping List is part of a family of apps owned by a company called Position Mobile. When you download the app it completely rearranges the entire Android's home screen because it is "a Launcher application" which is meant to make the app the default.

The privacy policy states upfront that the company's apps are supported by advertising. The app may share your information with advertisers or advertising networks. Those advertisers may also collect personal and non-personal information about you via cookies, beacons, pixels, and other technologies.

Recipes Home, compared to the other apps scrutinized for this report, was the most egregious in terms of advertising cookies and trackers. In fact, this app has so many advertising trackers that it made me wonder whether the app was created just for the purpose of collecting user data. Many trackers collected very detailed information about the device, including the phone's battery level, whether it was charging, and whether headphones were plugged in. One tracker, MoPub, was constantly requesting data from the device about ad auctions, how ads were performing, and how long the user paused on or scrolled through the ad.

Summary of user data collected

Tracker	Requests	Type	Data requested
MoPub	76	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, screen brightness, volume, orientation, language, connection type, battery level, battery status) - Ad identifiers (advertising identifier, device ID, consent data, ad group ID, whether the ad impression was served & cleared, ad auction info) - Location data (latitude/longitude)
Tapjoy	22	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen density, volume, language) - Ad identifiers (IDFA, advertising ID, analytics ID, ud ID, user, app group ID, managed device ID) - Location data
Facebook Graph	15	Advertising	- Device data (model, make, OS version,

			country, carrier, time zone) - Location data
Unity3D	3	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, screen brightness, volume, orientation, language, connection type, battery level, battery status, whether headphones connected, whether jailbroken) - Ad identifiers (info about the ad auction, history of user engagement with ads, AB testing group)
Google DoubleClick	2	Advertising	*N/A*
Yahoo	1	Advertising	- Device data (model, make, OS version, country, carrier, time zone) - Ad identifiers
Nexage	1	Advertising	*N/A*
Vungle	1	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, screen brightness, volume, orientation, language, connection type, battery level, battery status) - Ad identifiers (Android Ad ID, vdu ID)
Adjust	9	Advertising/ Analytics	- Ad identifiers (Ad ID)
Google Analytics	3	Analytics	*N/A*

Whisk

The award-winning cooking app Whisk is a “smart food platform” that matches a user’s recipe lists to local grocery stores based on preferences. It also connects with internet connected devices like smart fridges, using AI to identify what’s already in your fridge and suggest recipes with those ingredients. It was acquired by Samsung in 2019 with the goal of leveraging Samsung’s smart tech to “help businesses build integrated, intelligent, and meaningful food experiences for consumers.”

Whisk's privacy policy says that it shares your data with third parties, including partner companies like grocery stores, digital health apps, IoT tech vendors, and advertisers. Whisk also says that cookies are used in the app for retargeting ads.

We saw several advertising trackers collecting user data, most notably Braze, but otherwise trackers were relatively quiet.

Summary of user data collected

Tracker	Requests	Type	Data requested
Braze	23	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, time zone) - Ad identifiers (device ID) - Behavioral data
Facebook Graph	4	Advertising	- Device data (model, make, OS version, country, carrier, time zone) - Location data
Google DoubleClick	1	Advertising	*N/A*
MixPanel	15	Analytics	*N/A*
Google Analytics	3	Analytics	*N/A*

KptnCook

The KptnCook - Meal Planner, Recipes & Grocery List app is a recipe app, recently acquired by the company Miele, which is owned by German agriculture tech company Agrilution.

In the app's privacy policy, you can see a full list of third party service providers and advertisers who may have access to your data. The privacy policy also lays out exactly what pieces of user data are collected via the app, including detailed information about the end device and the Android Advertising ID or Apple IDFA.

To KptnCook's credit, the privacy policy is fairly thorough. Its list of third parties included not just trackers I identified in my observation of the app, but also a number of other trackers I didn't see. However, two of those trackers (Iterable and Branch) collect quite a lot of identifying information about you to help improve ad targeting and marketing.

Summary of user data collected

Tracker	Requests	Type	Data requested
Iterable	28	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, orientation, language, connection type) - Ad identifiers (email address, advertising ID, device ID, user ID, anonymous user ID) - Location data (latitude/longitude) - Behavioral data
Branch	6	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, orientation, language, connection type) - Ad identifiers (IDFA, Android Ad ID, Android ID, advertising IDs, Google Advertising ID, identity ID, device fingerprint ID, hardware ID) - Location data (latitude/longitude, locale)
Facebook Graph	6	Advertising	- Device data (model, make, OS version, country, carrier, time zone)
RevenueCat	2	Advertising	- Ad identifiers (AppsFlyer ID, whether user purchased subscription)
AppsFlyer	41	Advertising/ Analytics	*N/A*
MixPanel	11	Analytics	*N/A*

Crockpot Recipes

The app Crockpot Recipes: Healthy Recipes Crockpot Cooking appears to be owned by a company called Free Recipes Apps, but I can't find evidence of this company's existence online beyond a broken blog.

The app's privacy policy (which appears to be the only thing hosted on this blog) states that cookies are used for advertising and analytics. Not much else is disclosed about what data

is collected or how it is shared with third parties. Given the lack of any online presence for this company, I suspect the app was created simply to collect user data.

This hunch was confirmed when we observed app traffic: One advertising tracker, MoPub, was constantly serving ads and collecting information about the user's device and ad tracking IDs.

Summary of user data collected

Tracker	Requests	Type	Data requested
MoPub	57	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, screen brightness, volume, orientation, language, connection type, battery level, battery status) - Ad identifiers (advertising identifier, device ID, consent data, ad group ID, whether the ad impression was served & cleared, ad auction info) - Location data (latitude/longitude)
Google DoubleClick	8	Advertising	*N/A*
Google Analytics	2	Analytics	*N/A*

Flipp - Weekly Shopping

The Flipp - Weekly Shopping app is owned by Flipp Corporation, a "retail technology company" that works with brands to enhance their targeted advertising and marketing. The app sends you coupons and deals from businesses nearby, like grocery stores.

Given that the company supports the ad tech industry, I expected there to be a number of trackers running on the app. According to the app's privacy policy, the company works with advertising partners to deliver ads. User data is shared with analytics vendors, like Google Analytics. Third parties that do remarketing or ad targeting, like Google, Facebook, Braze, Branch, may collect detailed data about your device.

The privacy policy generally matched what I observed: Braze and Branch collected a lot of personal data, including a (fake) gmail address and various ad tracking IDs, like the Android Ad ID.

Summary of user data collected

Tracker	Requests for data	Type	Data requested
Braze	13	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, time zone) - Ad identifiers (device ID, email address) - Behavioral data
Facebook Graph	6	Advertising	- Device data (model, make, OS version, country, carrier, time zone)
Branch	4	Advertising	- Device data (model, make, OS version, country, carrier, screen resolution, screen size, orientation, language, connection type) - Ad identifiers (IDFA, Android Ad ID, Android ID, advertising IDs, Google Advertising ID, identity ID, device fingerprint ID, hardware ID) - Location data (latitude/longitude, locale)
Foursquare	1	Advertising/ Analytics	*N/A*
Google Analytics	5	Analytics	*N/A*

Conclusion

In our research, we observed a great deal of user data, including advertising IDs, being collected by Android apps. Many of these findings may come as no surprise: Cookies, beacons, pixels, and other tracking technologies are nearly impossible to avoid on the internet. The rapid growth in ad tech over the past two decades has resulted in an ever-expanding – and ever-consolidating – network of advertising, marketing, and analytics companies. (For a complete picture, check out this dizzying visualization of the industry by LUMAscapes). Our investigation into these Android apps confirms that third party tracking on mobile apps has ballooned out of control.

The responsibility for navigating this confusing privacy landscape should not fall on the consumer. While there are lots of things people can do to protect their privacy and prevent mobile ad tracking, trusted gatekeepers like Apple and Google need to do far more to protect consumers.

Apple, to its credit, has stepped up by requiring that users *opt in* to third party tracking through its new App Tracking Transparency feature in iOS 14.5. (However, enforcement of that feature is another story, as recent research has shown.)

On the other hand, Android's promise that users will be about to *opt out* of tracking simply doesn't go far enough. Most Android users will likely continue sharing data with third parties without realizing it. **This kind of 'tracking by default' is not a meaningful form of consent and Android needs to do more to protect people's privacy.**