FINDING PRIVACY-PROTECTIVE APPS

privacy policies

often hard to read due to complex language

ambiguous by design:

- we “may”…
- data collected could include…
- we do not share data with anyone beyond our affiliates*

* “affiliates” is defined to mean anyone with whom we share data.

privacy policies

assume:

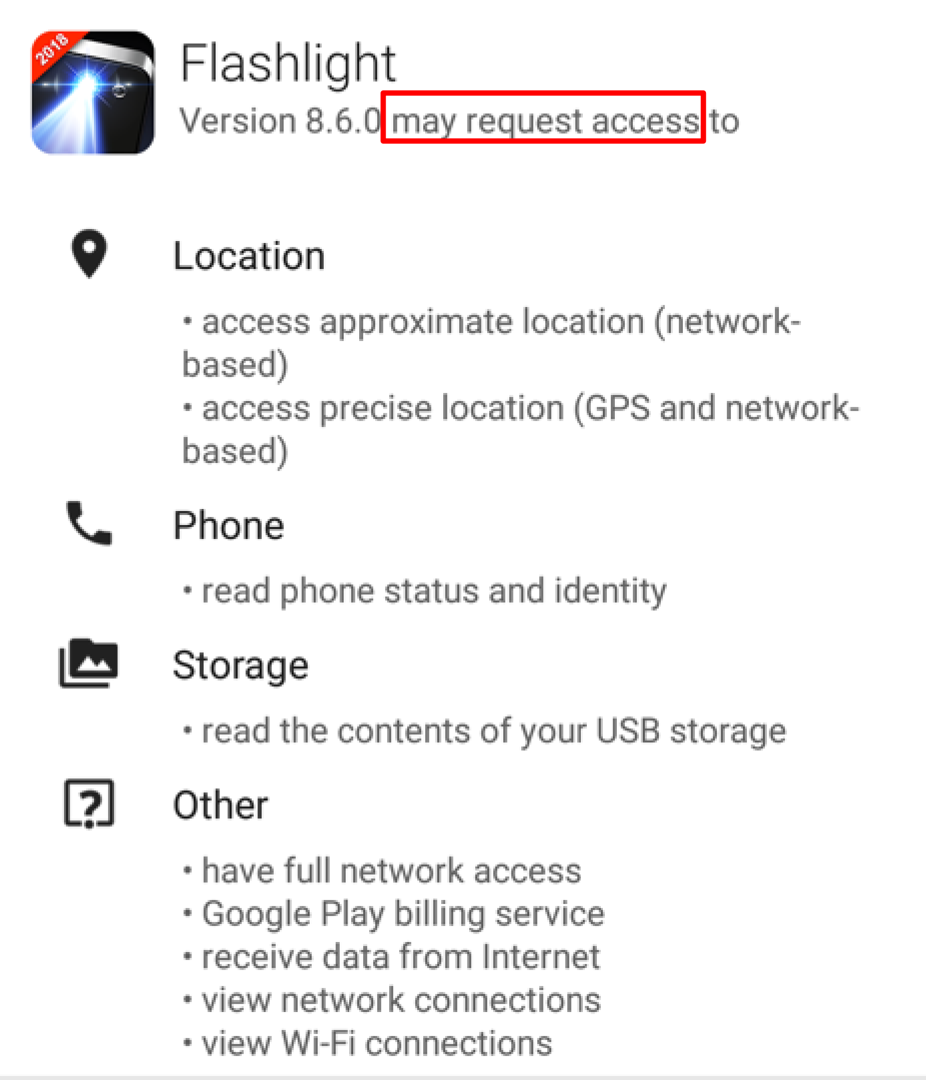
- an average reading rate of 250 words/minute
- the median policy has 2500 words
- an average of 100 unique websites visited/month

≈200 hours/year reading privacy policies

A. McDonald and L.F. Cranor. “The Cost of Reading Privacy Policies.”
In *I/S: A Journal of Law and Policy for the Information Society, 2008.*

Apps are able to request access to private user data and sensitive device resources.

In their app store listings (such as this one from the Google Play Store), apps disclose their capabilities. However, these disclosures don't tell the full story. Do apps actually use these privileges? With whom do they share sensitive data?



Flashlight

Version 8.6.0 may request access to

Location

- access approximate location (network-based)
- access precise location (GPS and network-based)

Phone

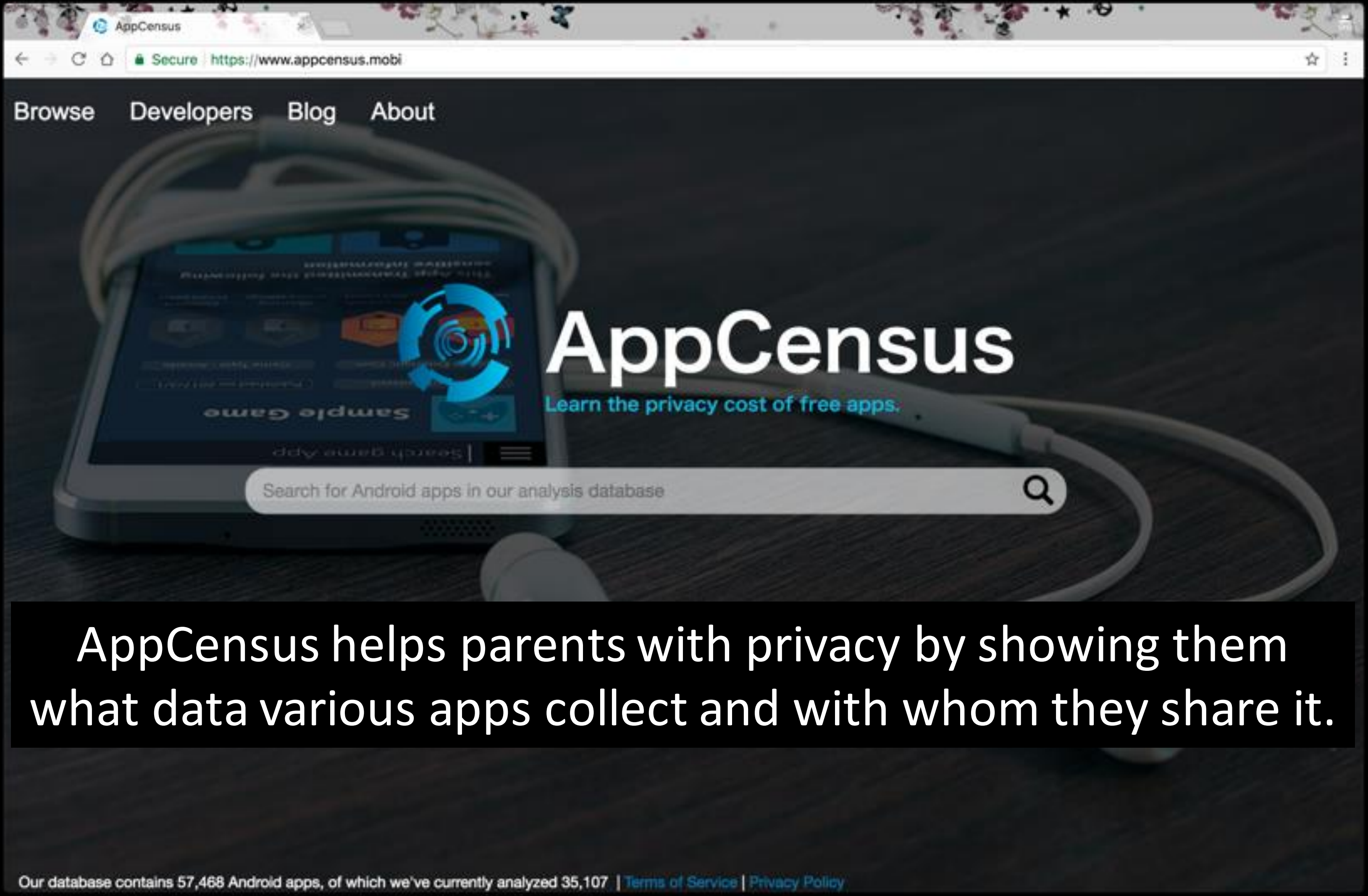
- read phone status and identity

Storage

- read the contents of your USB storage

Other

- have full network access
- Google Play billing service
- receive data from Internet
- view network connections
- view Wi-Fi connections



AppCensus

Learn the privacy cost of free apps.

Search for Android apps in our analysis database

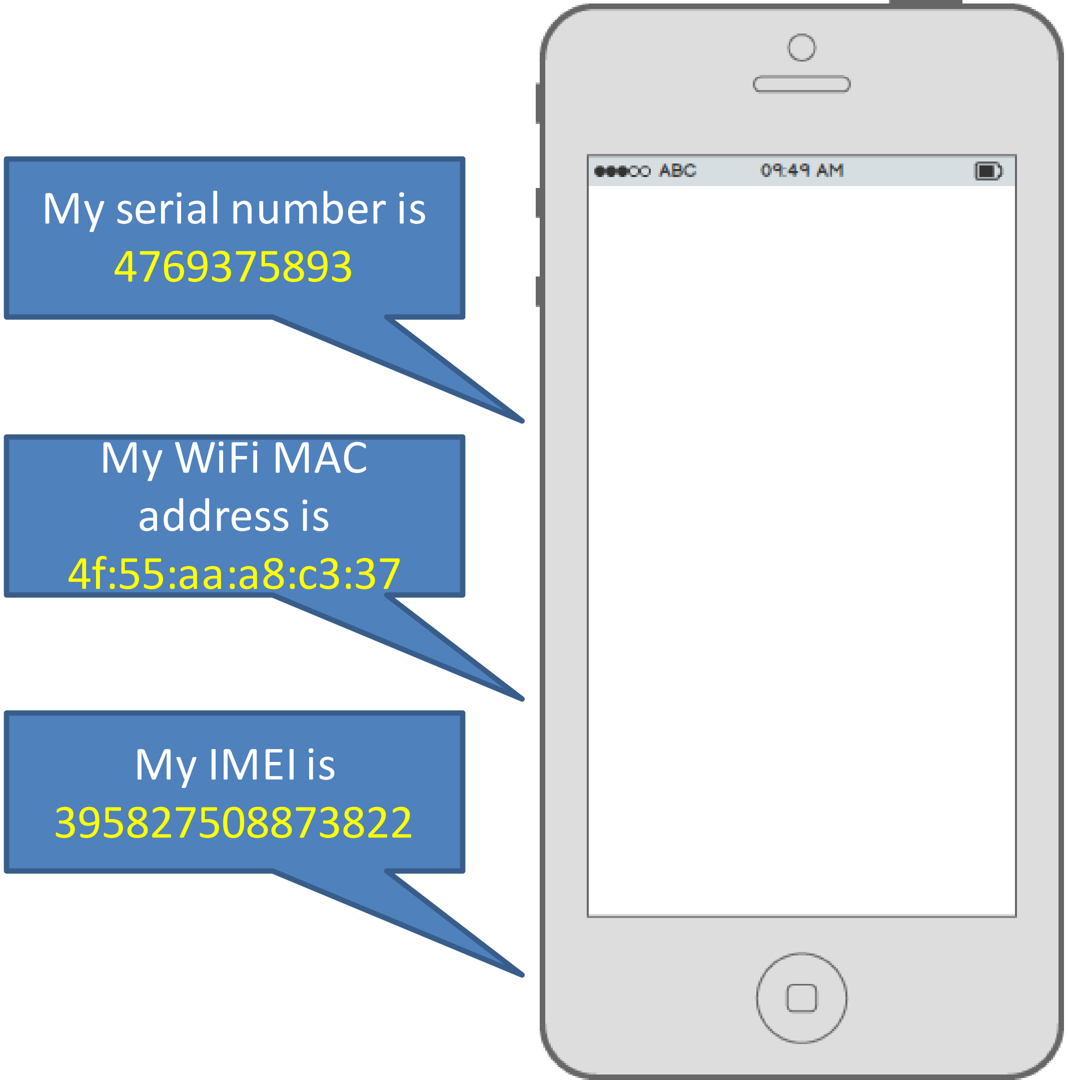
Our database contains 57,468 Android apps, of which we've currently analyzed 35,107 | Terms of Service | Privacy Policy

AppCensus helps parents with privacy by showing them what data various apps collect and with whom they share it.

MOBILE TRACKING EXPLAINED

Every device has several "persistent identifiers" that can be accessed by third-party apps.

A "persistent identifier" is a globally unique number.



My serial number is 4769375893

My WiFi MAC address is 4f:55:aa:a8:c3:37

My IMEI is 395827508873822

App developers get paid to share these identifiers with data brokers and advertising companies:

Serial number 4769375893 is playing Angry Birds

ACME Advertising

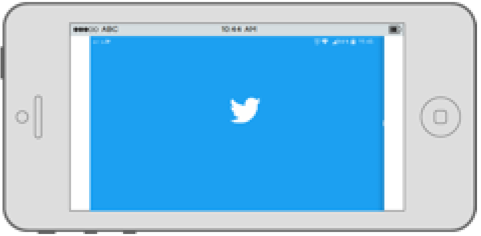
We now know that user with device serial number 4769375893 plays Angry Birds.

Using data received over time, third parties can use this data to build user profiles.

ACME Advertising

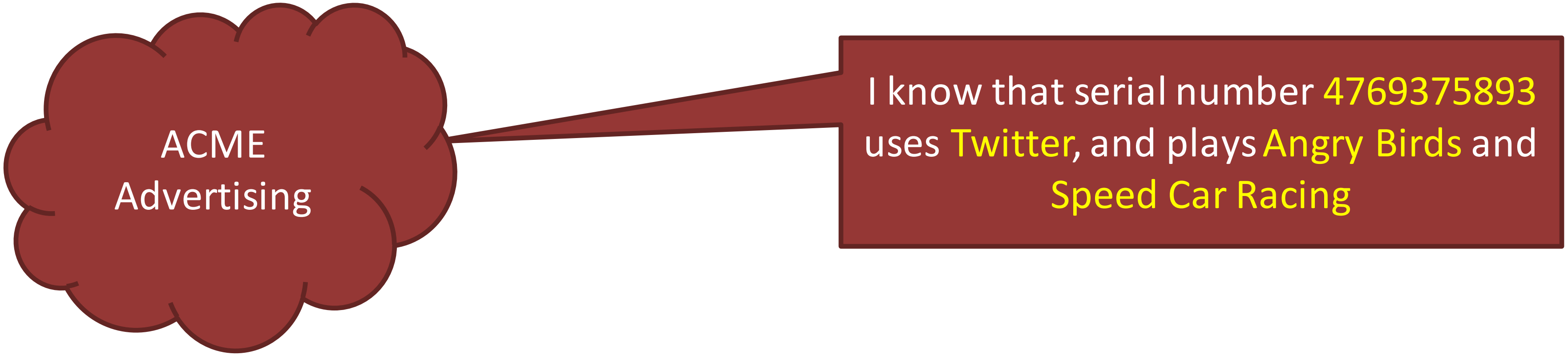
Serial number 4769375893 is playing Angry Birds

Serial number 4769375893 is using Twitter



Serial number 4769375893 is playing Speed Car Racing

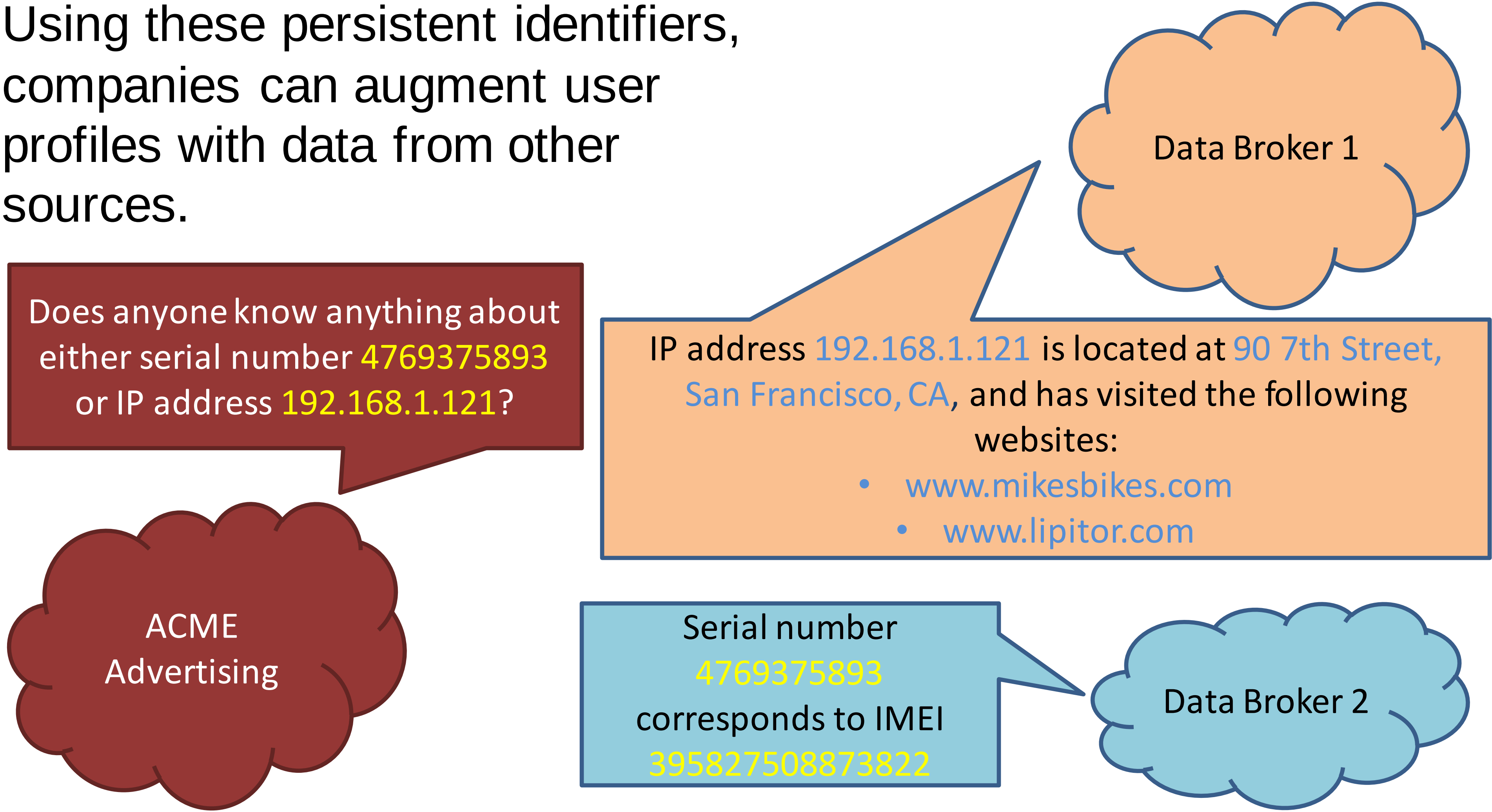
Using data received over time, third parties can use this data to build user profiles.



ACME Advertising

I know that serial number 4769375893 uses Twitter, and plays Angry Birds and Speed Car Racing

Using these persistent identifiers, companies can augment user profiles with data from other sources.



Does anyone know anything about either serial number 4769375893 or IP address 192.168.1.121?

ACME Advertising

Data Broker 1

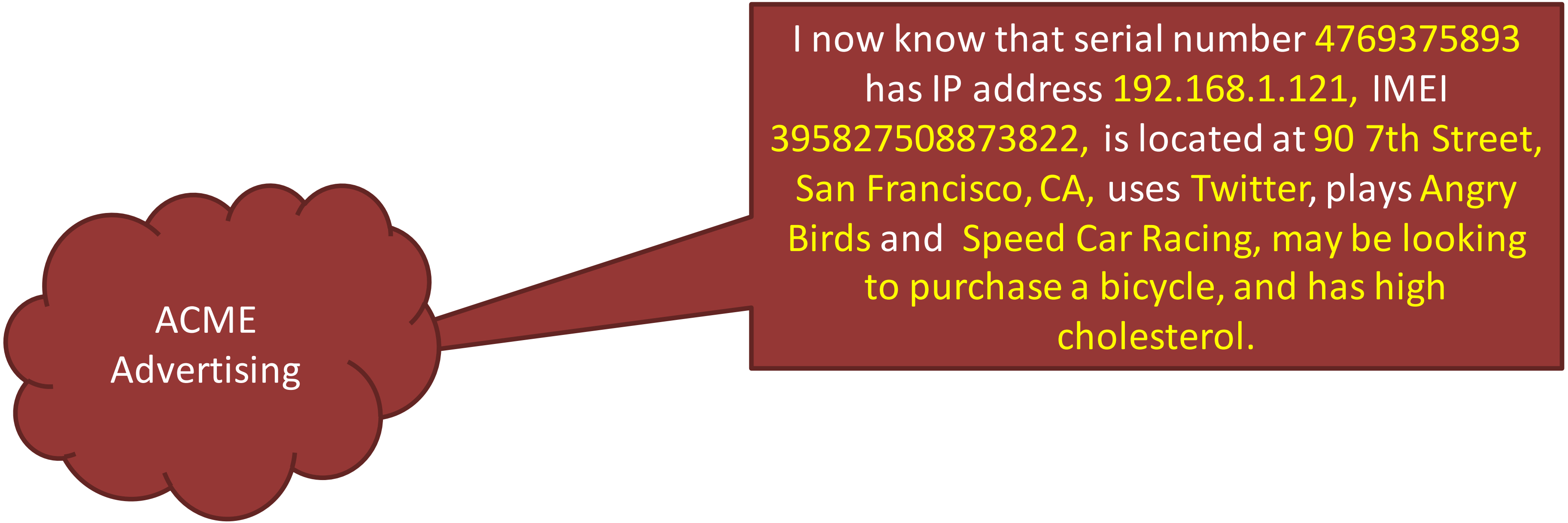
IP address 192.168.1.121 is located at 90 7th Street, San Francisco, CA, and has visited the following websites:

- www.mikesbikes.com
- www.lipitor.com

Data Broker 2

Serial number 4769375893 corresponds to IMEI 395827508873822

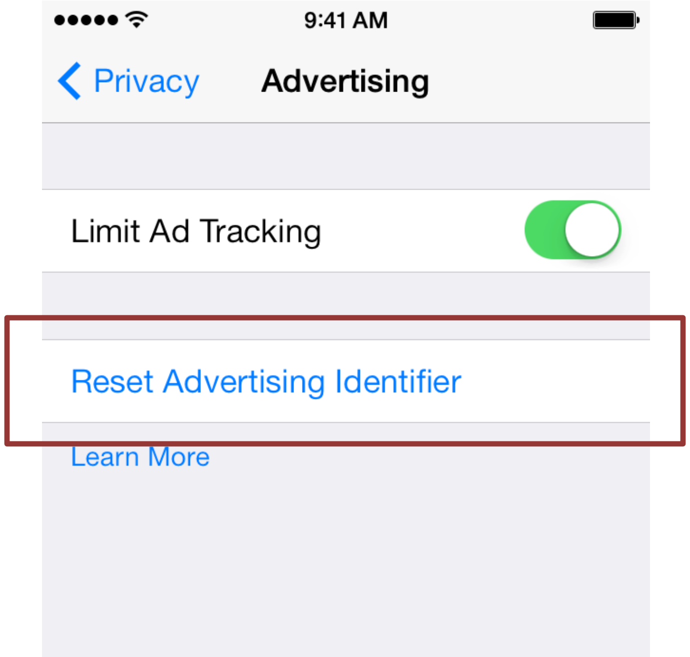
This allows them to build more detailed user profiles.



ACME Advertising

I now know that serial number 4769375893 has IP address 192.168.1.121, IMEI 395827508873822, is located at 90 7th Street, San Francisco, CA, uses Twitter, plays Angry Birds and Speed Car Racing, may be looking to purchase a bicycle, and has high cholesterol.

Both major mobile platforms (iOS and Android) introduced a user-resettable “ad ID” to prevent this sort of long-term tracking.

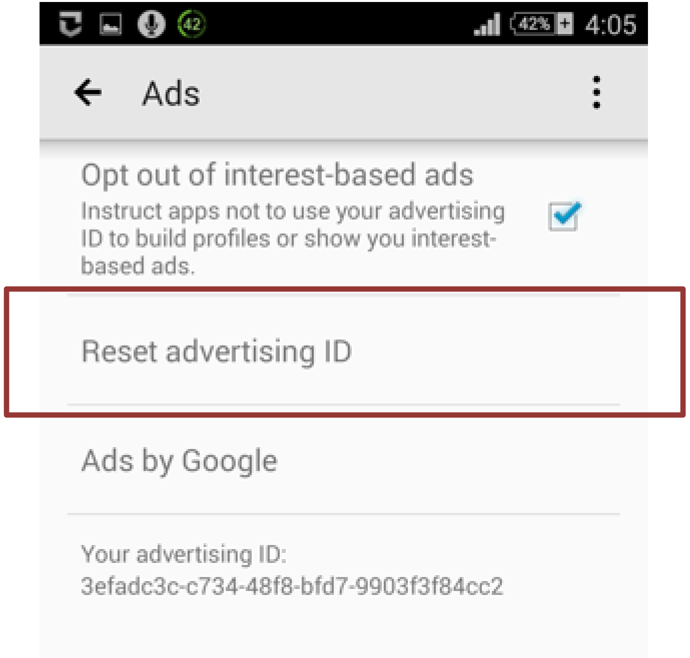


Advertising

Limit Ad Tracking ●

Reset Advertising Identifier

Learn More



Ads

Opt out of interest-based ads
Instruct apps not to use your advertising ID to build profiles or show you interest-based ads. ☑

Reset advertising ID

Ads by Google

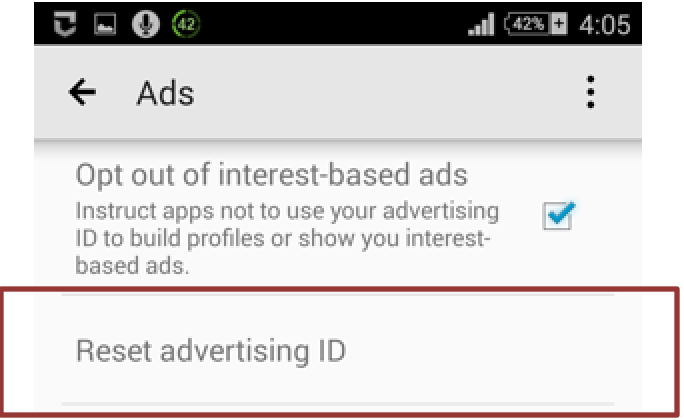
Your advertising ID:
3efadc3c-c734-48f8-bfd7-9903f3f84cc2

As of 2013, app developers on both iOS and Android are required to use this identifier in lieu of other persistent identifiers.

Android Ad ID 3efadc3c-48f8-bfd7-9903f3f84cc2 is playing Angry Birds

ACME Advertising

This privacy-protective feature is undermined if additional persistent identifiers are transmitted.



Ads

Opt out of interest-based ads ☑
Instruct apps not to use your advertising ID to build profiles or show you interest-based ads.

Reset advertising ID

Android Ad ID 48ae48bc-09ff-83e3-37592feb4c8a with IMEI 395827508873822 is playing Angry Birds

ACME Advertising

We have no profile for that AAID, **but** we do have a profile for IMEI 395827508873822

automatic behavior detection

what data goes to which parties?

is location data collected?

what persistent identifiers are collected?

- are they shared across apps?

The AppCensus system observes when apps access and share personal information, as well as unique persistent identifiers that can be used to track users over time and across services.

PERSONAL INFORMATION	PERSISTENT IDENTIFIERS
Owner Email Address	Hardware Serial Number
Phone Number	IMEI
GPS Latitude/Longitude	Wi-Fi MAC
Wi-Fi Router BSSID (MAC)	Android ID
Wi-Fi Router SSID (Name)	SIM Card ID
	Google Services Framework (GSF) ID
	Android Advertising ID (AAID)

57% of “Designed for Families” apps are in potential violation

POTENTIAL VIOLATION	RATE (n=5,855)
Personal information	4.8%
Non-resettable identifiers	39%
Potentially non-compliant services	19%
Failure to take security measures	40%

Note that some apps were observed engaging in more than one of these behaviours, so the percentages will add up to more than 57%.

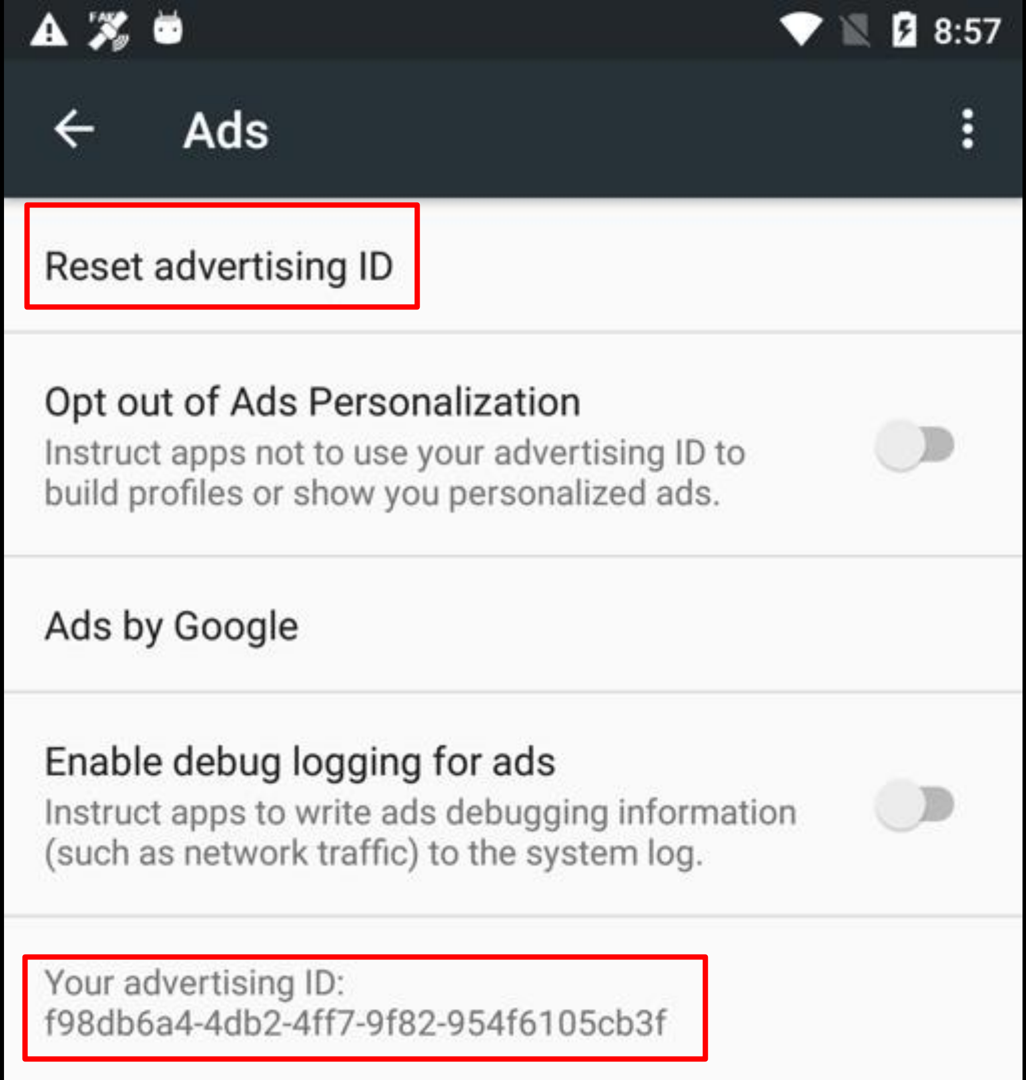
potential violations often arise from third-party services included with apps

These services allow developers to expedite production by offering drop-in functionality (eg. graphics, communications, advertising, or analytics)

potential violations persist
due to platform providers not
enforcing their own terms

Behavioural advertising uses persistent identifiers to build profiles of users by tracking individuals over time and across services.

Google has recognised the privacy implications of persistent identifiers, and in 2014 introduced the resettable Android Advertising ID (AAID) to give users (or parents) control over how advertisers track them. Google requires developers and advertisers to use this in lieu of non-resettable device identifiers like the IMEI and Wi-Fi MAC address.



8:57

Ads

Reset advertising ID

Opt out of Ads Personalization
Instruct apps not to use your advertising ID to build profiles or show you personalized ads.

Ads by Google

Enable debug logging for ads
Instruct apps to write ads debugging information (such as network traffic) to the system log.

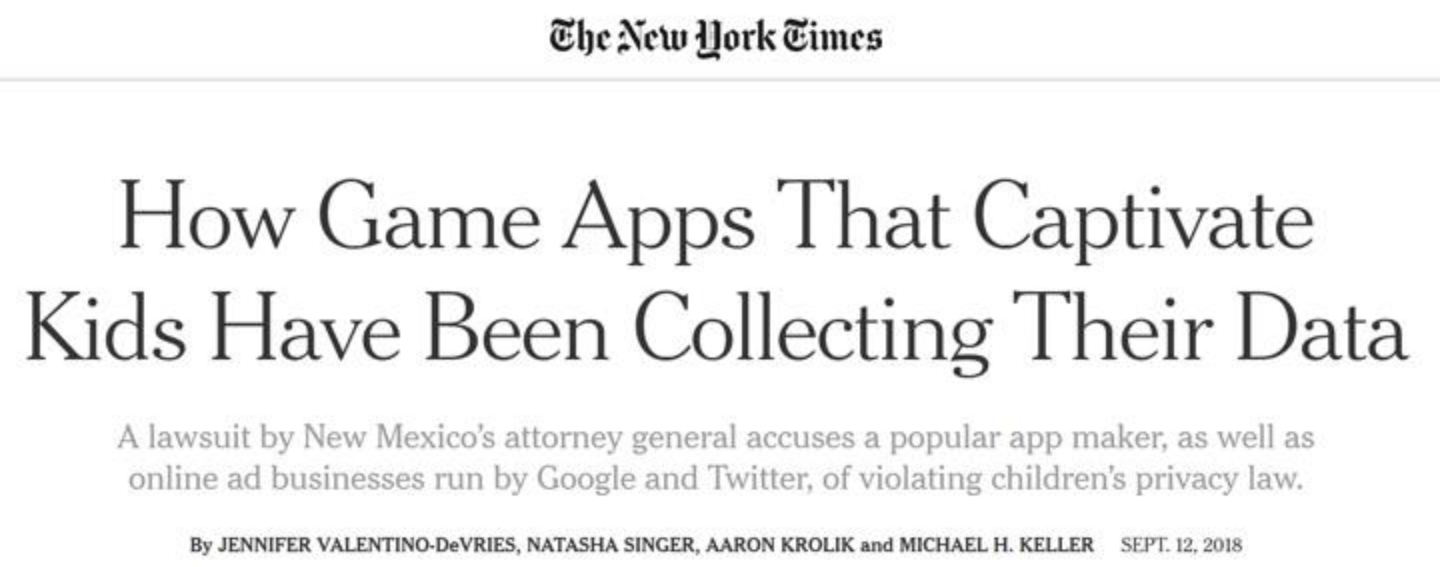
Your advertising ID:
f98db6a4-4db2-4ff7-9f82-954f6105cb3f

75% of apps transmitting the ad ID do so alongside other persistent identifiers.

this negates the privacy-preserving behaviors of the ad ID (and violates Google’s terms).

19% share identifiers or personal information with services not allowed in children’s apps

In September 2018, the New Mexico Attorney General filed a suit, with Tiny Lab Productions and Google as co-defendants for violating children's privacy law.



The New York Times

How Game Apps That Captivate Kids Have Been Collecting Their Data

A lawsuit by New Mexico's attorney general accuses a popular app maker, as well as online ad businesses run by Google and Twitter, of violating children's privacy law.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, AARON KROLIK and MICHAEL H. KELLER SEPT. 12, 2018

https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html

After facing scrutiny from the New York Times and the New Mexico AG's office, Google recently took a more aggressive stance towards Tiny Labs, taking down their apps after Tiny Labs failed to address the various privacy issues we identified in those products.

These slides were selected by ACCM from the following presentation:

Won’t Somebody Think of the Children?!

Examining Privacy Behaviors of Mobile Apps at Scale

Serge Egelman
egelman@cs.berkeley.edu
@v0max

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Berkeley
UNIVERSITY OF CALIFORNIA

Source:
https://d1oclgbf4bbu9h.cloudfront.net/wp-content/uploads/2018/12/Copy-of-Egelman.