Examining Privacy Violations in Children's Apps

Irwin Reyes, **Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman**

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Berkeley
UNIVERSITY OF CALIFORNIA

UBC
THE UNIVERSITY OF BRITISH COLUMBIA

UNIVERSITY OF CALGARY

Stony Brook University

imdea networks

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

automated run-time analysis to observe
how apps **actually access and share** data

I. Reyes, P. Wijesekera, J. Reardon, A. Elazari Bar On, A. Razaghpanah, N. Vallina-Rodriguez, S. Egelman. *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, Privacy Enhancing Technologies Symposium (PETS) 2018

Available at https://appcensus.mobi/about

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)

US Children's Online Privacy Protection
COPPA

personal information

behavioral advertising **X**

verifiable parental consent ✔

reasonable security measures ✔

FINES UP TO 40K USD PER VIOLATION

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC   **NEWS & EVENTS**   **ENFORCEMENT**   **POLICY**   **TIPS & ADVICE**

Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act

Companies' Apps Shared Kids' Information with Ad Networks; Will Pay $360K In Civil Penalties

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC | **NEWS & EVENTS** | **ENFORCEMENT** | **POLICY** | **TIPS & ADVICE**

Home » News & Events » Press Releases » Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Mi Permission

Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission

Company Will Pay $950,000 For Tracking Children Without Parental Consent

Google Play

Search

Apps

My apps

Shop

Games

Family

Editors' Choice

| Categories ⌄ | **Home** | Top Charts | New Releases |

Daydream	Games	Family
Art & Design	Action	Ages 5 & Under
Auto & Vehicles	Adventure	Ages 6-8
Beauty	Arcade	Ages 9 & Up
Books & Reference	Board	Action & Adventure
Business	Card	Brain Games
Comics	Casino	Creativity
Communication	Casual	Education
Dating	Educational	Music & Video
Education	Music	Pretend Play

8

Designed for Families

☐ Opt in to Designed for Families

Designed for Families is a developer program for apps and games designed specifically for children and family audiences. Learn More

Eligibility

All apps participating in the Designed for Families program must be relevant for children under the age of 13 and comply with the eligibility criteria below. App content must be appropriate for children. Google Play reserves the right to reject or remove any app determined to be inappropriate for the Designed for Families program.

7. You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule) and other relevant statutes including any APIs that your app uses to provide the service.

https://play.google.com/about/families/designed-for-families/program-requirements/

5,855 free "Designed for Families" apps

57% of "Designed for Families" apps are in potential violation

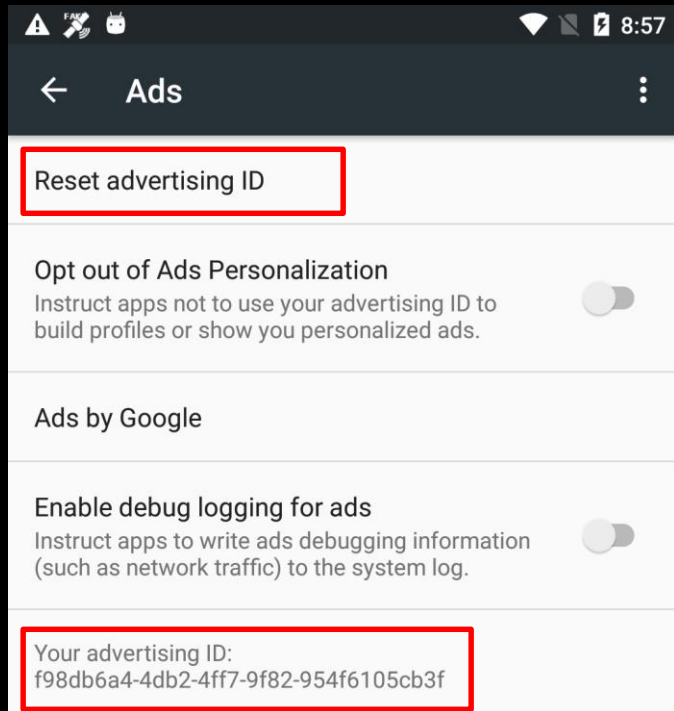| POTENTIAL VIOLATION	RATE (n=5,855)
Personal information	4.8%
Non-resettable identifiers	39%
Potentially non-compliant services	19%
Failure to take security measures	40%

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

**potential violations persist
due to platform providers not enforcing terms**

Policy requirements

The Google Play Developer Program Policy ⧉ requires that all updates and new apps uploaded to Google Play use the advertising ID (when available on a device) in place of any other device identifiers for any advertising purposes. You're responsible for ensuring your apps are in compliance with policies regarding its usage, as well as all Play policies.

Apps using a persistent ID other than the advertising ID may receive a policy violation warning via the publisher site or the email address used to register the account. If you receive a warning, you should ensure that any published APKs comply with the advertising ID related guidance in the Developer Program Policy ⧉. If you are using a third-party ad SDK, please contact the SDK maker to obtain a new version that complies with this new policy.

← **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

39% **share the AAID along another identifier, negating its privacy preserving benefits**

AD PLATFORM	VIOLATION OF IDENTIFIER POLICY
Chartboost	> 99%
GreedyGame	> 99%
Tapjoy	98%
…	…
mopub	3%
LKQD	2%
DoubleClick by Google	1%
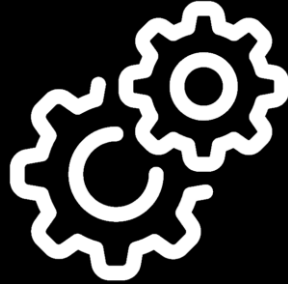
19% share identifiers or personal information with **services not allowed in children's apps**

not for children's apps

crashlytics

Developer further agrees it will not integrate the Software into any Application or Beta Application (i) with end users who Developer has actual knowledge are under the age of 13, or (ii) that may be deemed to be a "Web site or online service directed to children" as defined under the Children's Online Privacy Protection Act of 1998 ("COPPA") and the regulations promulgated thereunder.

Crashlytics

From Wikipedia, the free encyclopedia

Crashlytics is a Google-owned Boston, Massachusetts-based software company founded in May 2011 by entrepreneurs Wayne Chang and Jeff Seibert.

industry self-regulation via safe harbors has had no measurable positive effect

POTENTIAL VIOLATION	DFF (n=5,855)	SAFE HARBOR (n=237)
PERSONAL INFO	4.8%	10%
NON-RESETTABLE IDENTIFIERS	39%	39%
PROHIBITED SERVICES	19%	33%
NO BASIC SECURITY MEASURES	40%	49%

industry and regulators react

Fun Kid Racing

Tiny Lab Racing Games   Racing   Action & Adventure   ★ ★ ★ ★ ★ 79,028 👤

E Everyone

Contains Ads · Offers in-app purchases

⚠ You don't have any devices

Add to Wishlist   Install

The app's developers, Tiny Lab Productions, said in an email that its apps are "directed for families," and not children, because "we see that grownups and teens plays our games." - CNET

tinylabproductions.com
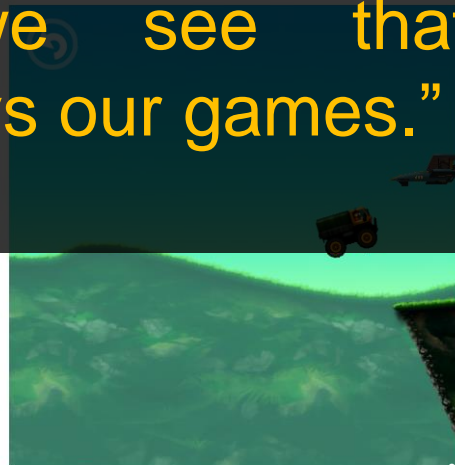
TINY LAB
PRODUCTIONS

GAMES   ABOUT US   PRESS   CAREERS   KIDS

RACING GAME FOR KIDS

CHILDREN LOVE IT!

Fun Kid Racing is one of the best racing games for kids — this free game features simple controls that children love and can quickly master. Take control of a huge variety of vehicles and race them to the finish line, optionally collect coins along the way, and do fun stunts on the many varied environments.

The levels are designed specifically for children, and will keep them entertained for hours!

Google play   Windows Phone

We have identified that 2,667 apps are potentially incorrectly listed as directed to "mixed audiences," and "not primarily directed to children," corresponding to ~51% of Designed for Families (DFF) apps from our original sample which are still listed on DFF. Developers seem to have an incentive to miscategorize their apps as "not primarily directed to children" so they will be able to engage in defective "age gating," thereby very likely causing children under 13 to enter ages over 13, allowing COPPA-prohibited behavioral advertising.

Email from our team to Google

115.   In response, Google offered two primary rebuttals: (1) there was no mechanism to detect and prevent the issue "at scale"; and (2) more information was required on appropriate "heuristics" to support the conclusion that the Tiny Lab apps at issue were child directed.

tinylabproductions.com

GAMES ABOUT US PRESS CAREERS KIDS

RACING GAME FOR KIDS

CHILDREN LOVE IT!

Fun Kid Racing is one of the best racing games for kids — this free game features simple controls that children love and can quickly master. Take control of a huge variety of vehicles and race them to the finish line, optionally collect coins along the way, and do fun stunts on the many varied environments.

The levels are designed specifically for children, and will keep them entertained for hours!

Google play

Windows Phone

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

A month later, Google appeared to reverse course: The company told Mr. Abromaitis it had identified a Tiny Lab app that should be designated for children. Google gave Tiny Lab a week to change that app and any others like it. Tiny Lab labeled 10 of its apps for children and used ad networks in them designed for children's apps. Google approved the updates but flagged more apps at the end of August, Mr. Abromaitis said, so he made another round of changes.

Then, this week, after inquiries from The Times, Google terminated Tiny Lab's account and removed all of its apps from the Play store, citing multiple policy violations.

closing recommendations

regulators: examine the gatekeepers

platform providers: stricter security and analysis

app developers: use compliant services

parents: ¯_(ツ)_/¯

https://appcensus.mobi

BACKUP

https://api.wigle.net/swagger#!/Network_search_and_information_tools/detail

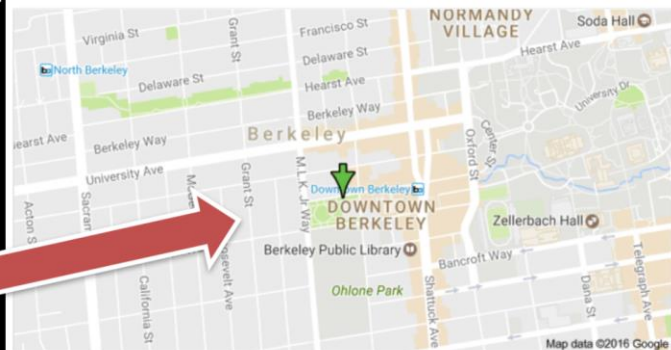| Parameter	Value	Descriptio...
netid	38:1c:1a:c4:ba:b0	The WiFi search

Response Body

```
{
  "gsm": false,
  "wifi": true,
  "success": true,
  "cdma": false,
  "results": [
    {
      "trilat": 37.86978912,
      "trilong": -122.27120972,
      "ssid": "ICSI",
```

37.86978912,-122.27120972

All   Maps   Videos   Shopping   Images   More   Settings   Tools

About 0 results (0.40 seconds)

NORMANDY VILLAGE   Soda Hall
North Berkeley
Virginia St   Grant St   Francisco St   Delaware St   Hearst Ave   University Dr
Delaware St   Hearst Ave
Berkeley Way   Berkeley
Hearst Ave   Berkeley Way   Oxford St   Center St
University Ave   Downtown Berkeley   DOWNTOWN BERKELEY   Zellerbach Hall
Acton St   Sacramento St   Grant St   M.L.K Jr Way   Berkeley Public Library   Bancroft Way
Ohlone Park   California St   Roosevelt Ave   Shattuck Ave   Durant Ave   Telegraph Ave
Map data ©2016 Google

Map for 37.86978912,-122.27120972

DOMAIN	APPS SENDING IDs	APPS SENDING NON-AAID IDs	COMPLIANCE WITH GOOGLE POLICY
doubleclick.net	168	1	99%
lkqd.net	65	1	98%
mopub.com	148	3	97%
…	…	…	…
adcolony.com	557	108	80%
supersonicads.com	465	144	69%
tapjoy.com	98	96	2%
tapjoyads.com	95	94	1%
chartboost.com	859	858	< 1%
greedygame.com	59	59	< 1%

ROUTER MAC SENT TO DOMAIN	APP COUNT
greedygame.com	61
startappservice.com	60
startappexchange.com	57
kochava.com	30
app-nxt.net	13

2,909 apps used Unity (from DFF corpus of 5,855)

1,068 received "coppaCompliant" flag from Unity server

479 have coppaCompliant=true

589 have coppaCompliant=false

1,280 apps integrated with Facebook (from DFF corpus of 5,855)
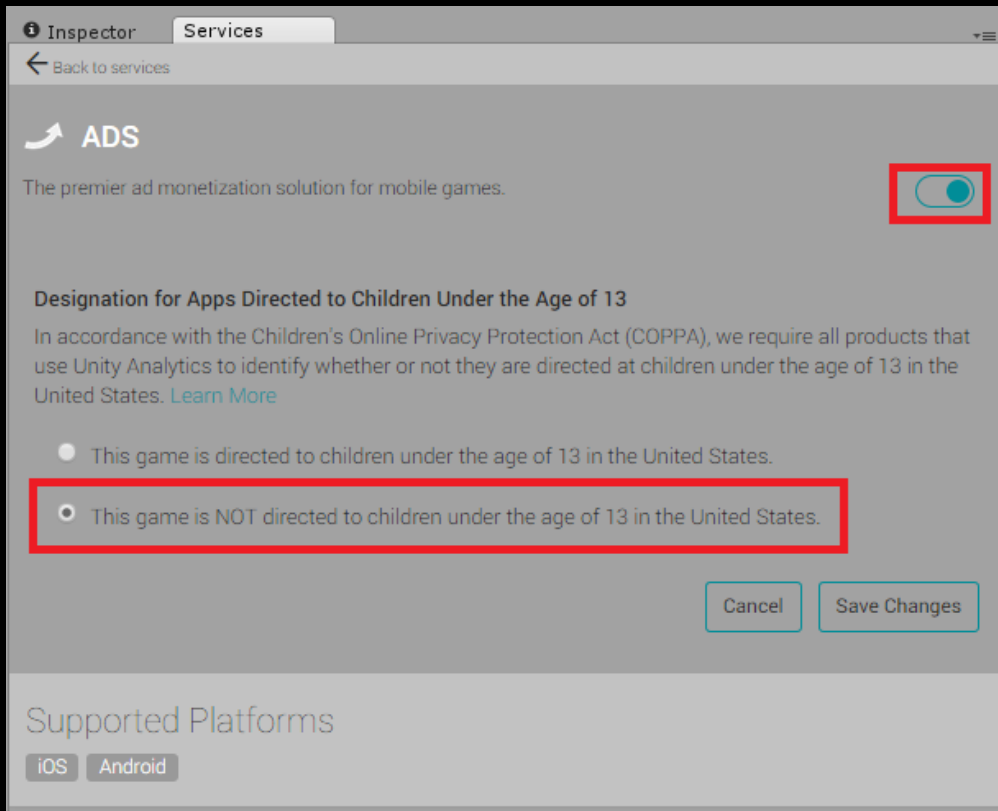
444 sent "coppa" flag to Facebook server

75 have coppa=true

342 have coppa=false

27 have coppa=true and false (both!)

Supply Partners who sign up using this website may not provide MoPub with data from end users under age 13. Supply Partners must not register for MoPub's services using this website if any of their apps are either: (1) directed to children under age 13 (even if children are not the app's primary audience), or (2) collect information from children that Supply Partners know are under age 13.

- MoPub Terms of Service

← Back to services

➚ ADS

The premier ad monetization solution for mobile games.

Designation for Apps Directed to Children Under the Age of 13

In accordance with the Children's Online Privacy Protection Act (COPPA), we require all products that use Unity Analytics to identify whether or not they are directed at children under the age of 13 in the United States. Learn More

○ This game is directed to children under the age of 13 in the United States.

● This game is NOT directed to children under the age of 13 in the United States.

Cancel   Save Changes

Supported Platforms

iOS   Android

supersonic

CHI... ...LICY

The Se... ...der the... ...use any po... ...does n... collected online from children under the age of 13, to the extent prohibited by the Children's Online Privacy Protection Act. Nor do we knowingly create profile segments of children under 13 years of age. If you believe

Androbaby

BabyBus Kids Games

41

Pop Girls - High School Band

TabTale **Casual** **Pretend Play**

★ ★ ★ ★ ★ 24,974 👤

E Everyone

Contains Ads · Offers in-app purchases

⚠️ You don't have any devices.

🔖 Add to Wishlist

Install

Dress up in style!

Watch out pop divas!

	DFF APPS (n=5,855)	SAFE HARBOR APPS (n=237)
SEND IDENTIFIERS	73%	66%
SHARE PERSONAL DATA	4.8%	10%
USE VERBOTEN SDK	19%	33%
DON'T ENCRYPT COMMS	40%	49%

custom android for
logging api calls

+
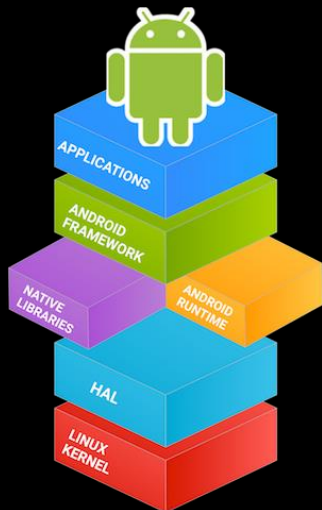
lumen app for
network flow analysis

P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, K. Beznosov, *The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*, IEEE Security and Privacy (Oakland) 2017

A. Razaghpanah, R. Nithyanand, N. Vallina Rodriguez, Srikanth Sundaresan, M. Allman, C. Kreibich, P. Gill, *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*, Network and Distributed System Security (NDSS) 2018

dynamic analysis environment

any Android app

input event generator to explore the app

observed app behavior

what was accessed

where it was shared
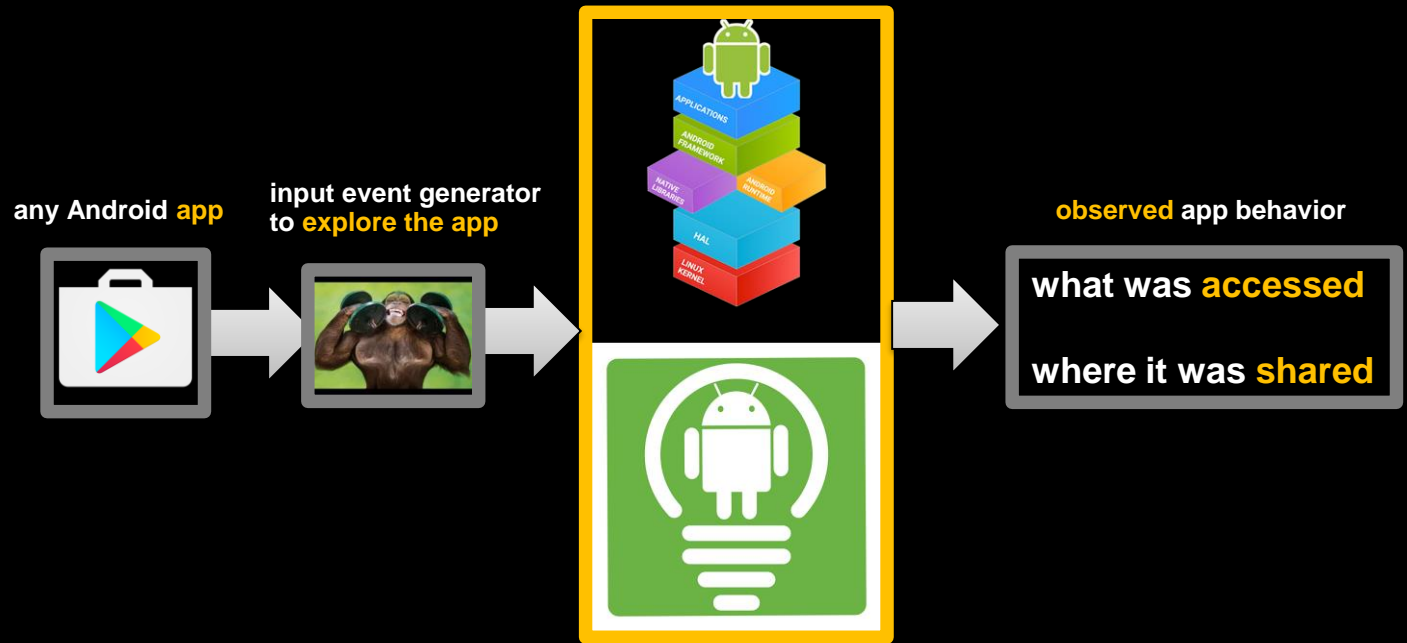
current deployment runs 1,000 apps/day

📋 Platforms   📊 Statistics   🔧 **Settings**   ❓ Instructions

PROJECT OVERVIEW

This is a short project overview that contains information that you might need wh

Project details can be edited in Unity Connect, click here to open it in a new tab.

Project ID: f8ede587-8091-48d5-aaff-986995bb4915

Coppa

☑ This game is directed to children under the age of 13 in the United States

Learn more about COPPA

50% used Unity (from DFF corpus of 5,855)

84% of Unity apps did NOT get coppaCompliant=true

SDK	TOTAL DFF INSTALLS
crashlytics	556M
supersonic + ironSource	481M
Tapjoy	386M
mopub	296M
INNERACTIVE	239M
heyZap	150M

40% share identifiers and personal info
without using encrypted HTTP

Overall, 57% of "Designed for Families" apps are in potential violation