“Won’t Somebody Think of the Children?”
Examining COPPA Compliance at Scale

CRYPTO & PRIVACY VILLAGE

DEF CON 26

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

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

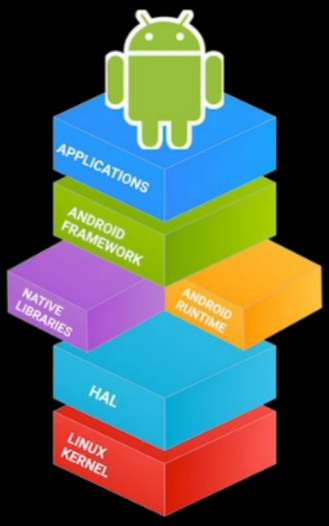
- read the contents of your USB storage

Other

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

dynamic analysis platform to observe how apps actually access and share data

custom android for logging api calls



+

lumen app for network flow analysis

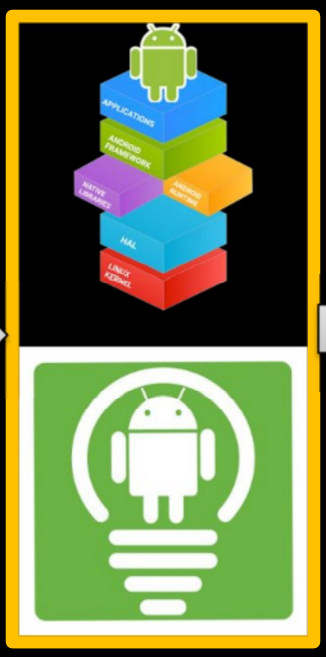
P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, K. Beznosov, *The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*, IEEE Security and Privacy (Oakland) 2017

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

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)


Are you familiar with COPPA? Who?

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Conn

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

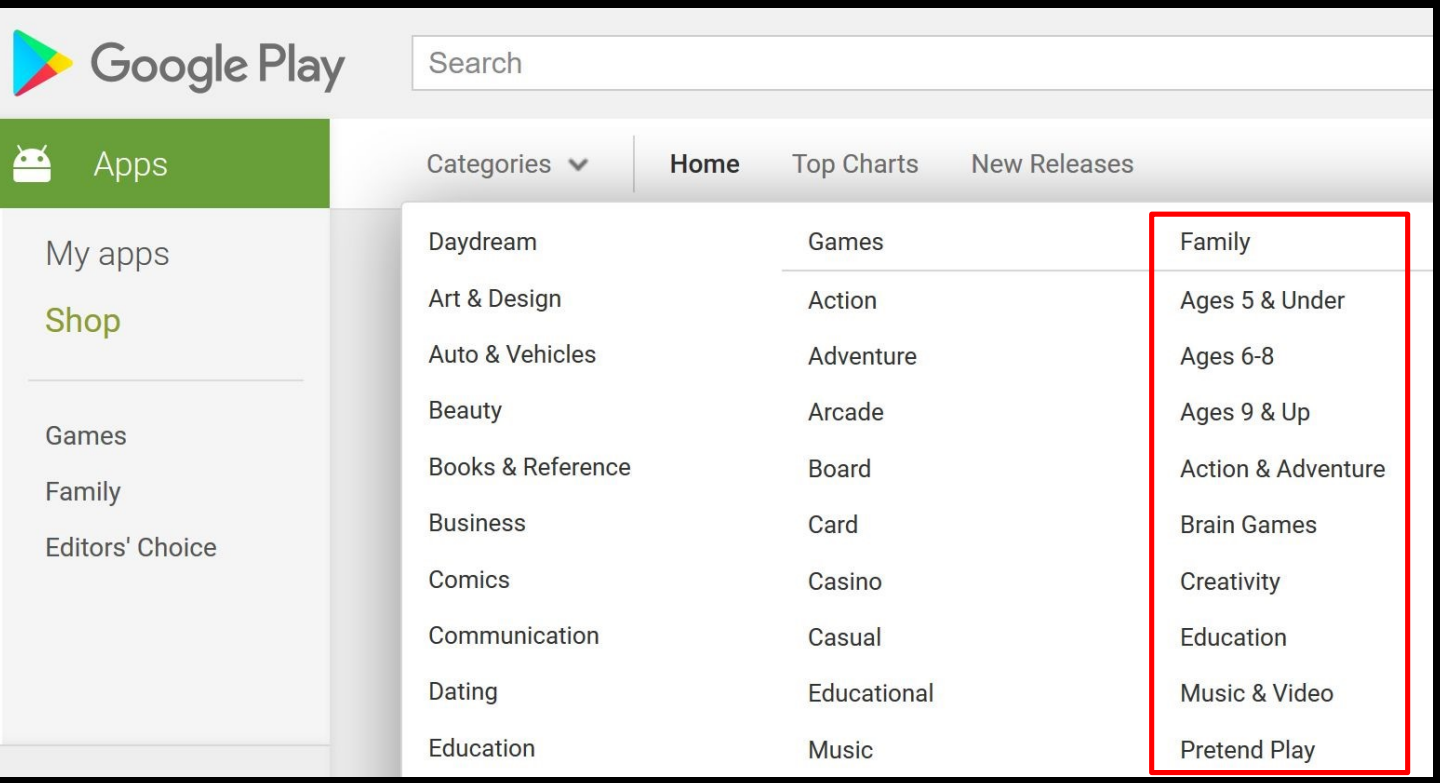
COPPA applies to:

✔ **Operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children.**

✔ **Operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13.**

✔ **Websites or online services (third parties) that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.**

https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions


Google Play
Search
Apps
Categories
Home
Top Charts
New Releases
My apps
Shop
Games
Family
Editors' Choice
Daydream
Art & Design
Auto & Vehicles
Beauty
Books & Reference
Business
Comics
Communication
Dating
Education
Games
Action
Adventure
Arcade
Board
Card
Casino
Casual
Educational
Music
Family
Ages 5 & Under
Ages 6-8
Ages 9 & Up
Action & Adventure
Brain Games
Creativity
Education
Music & Video
Pretend Play

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.

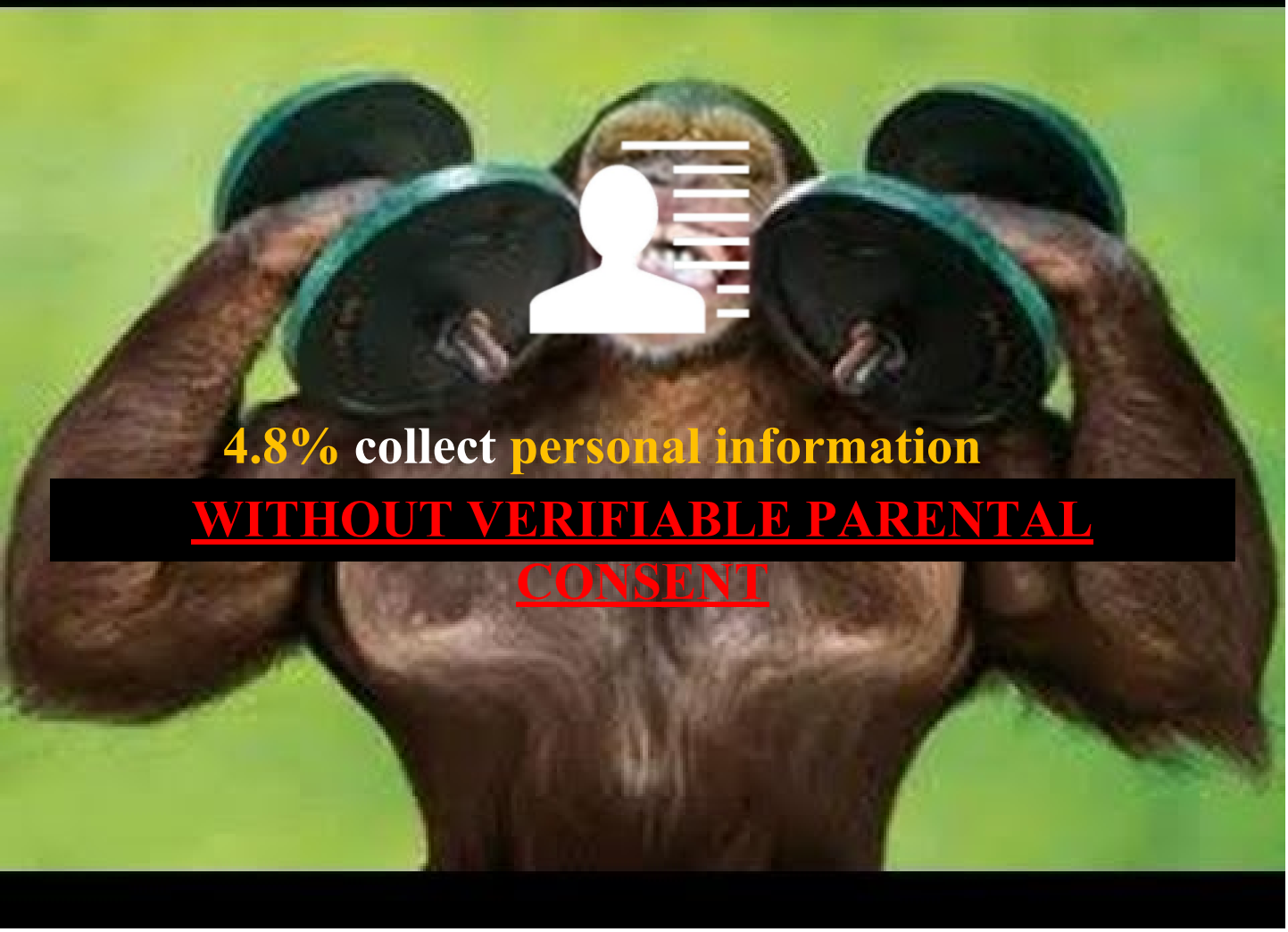
7. You represent that apps submitted to Designed for Families are compliant with COPPA (Children's Online Privacy Protection Rule) and other relevant statutes including any APIs that your app uses to provide the service.

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 SDKs	19%
Failure to take security measures	40%


4.8% collect personal information
WITHOUT VERIFIABLE PARENTAL CONSENT

KOCHAVA

STARTAPP

mopub

skydeo

4.4% collect fine geolocation data

appnext

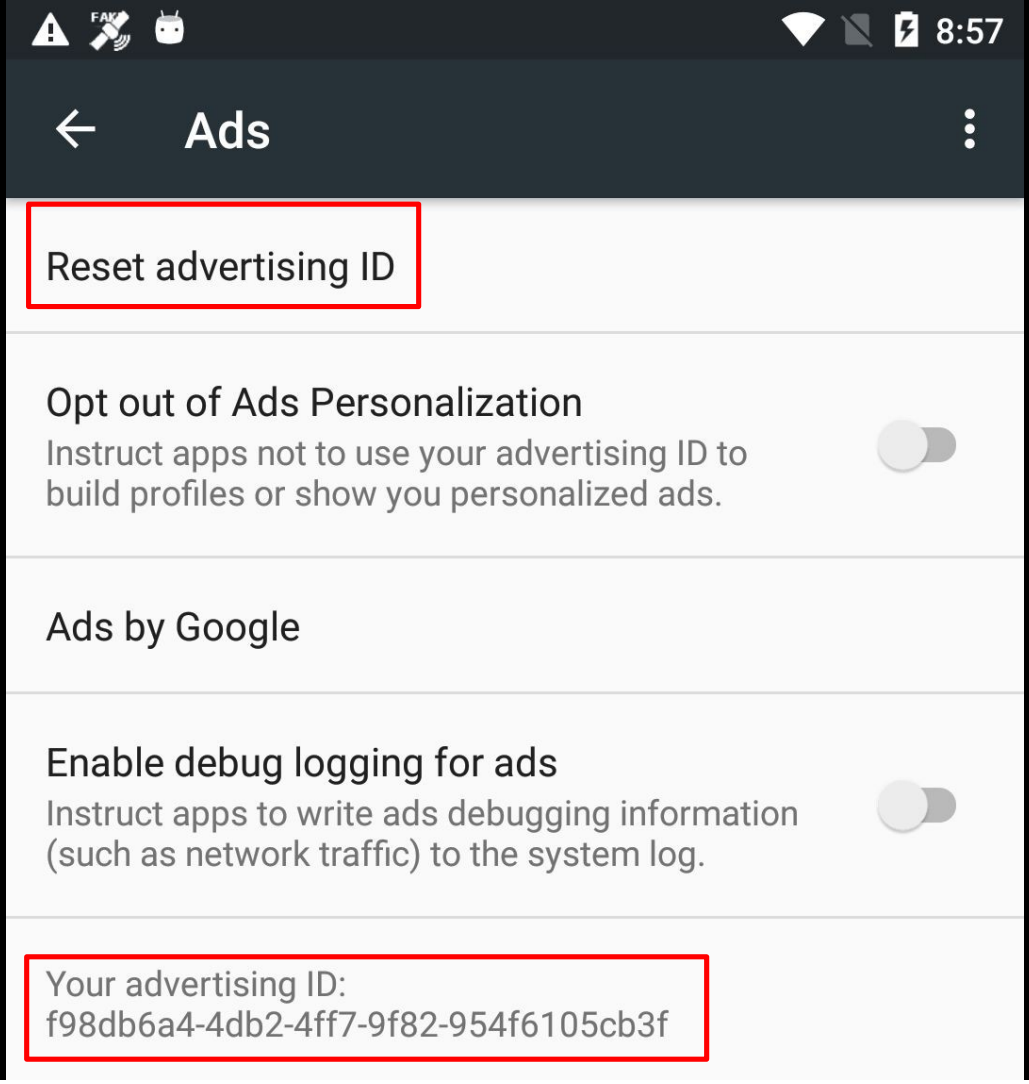
INNERACTIVE

AERSERV

Greedy Game

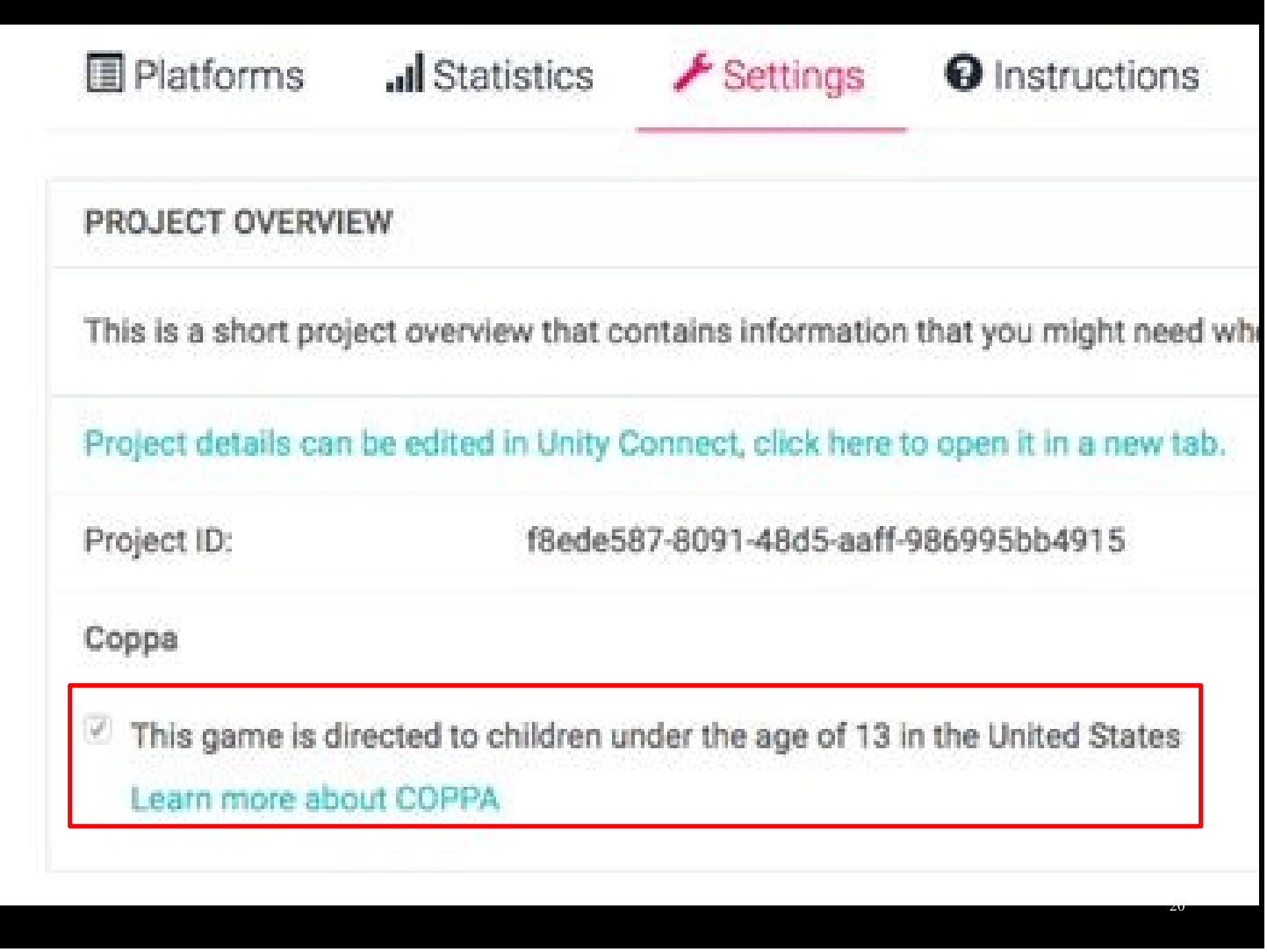
1.9% collect **contact information**

skydeo


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

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

AD PLATFORM	VIOLATION OF IDENTIFIER POLICY
Chartboost	> 99%
Greedy Game	> 99%
Tapjoy	98%
…	…
mopub	3%
LKQD	2%
DoubleClick by Google	1%


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

not for children's apps

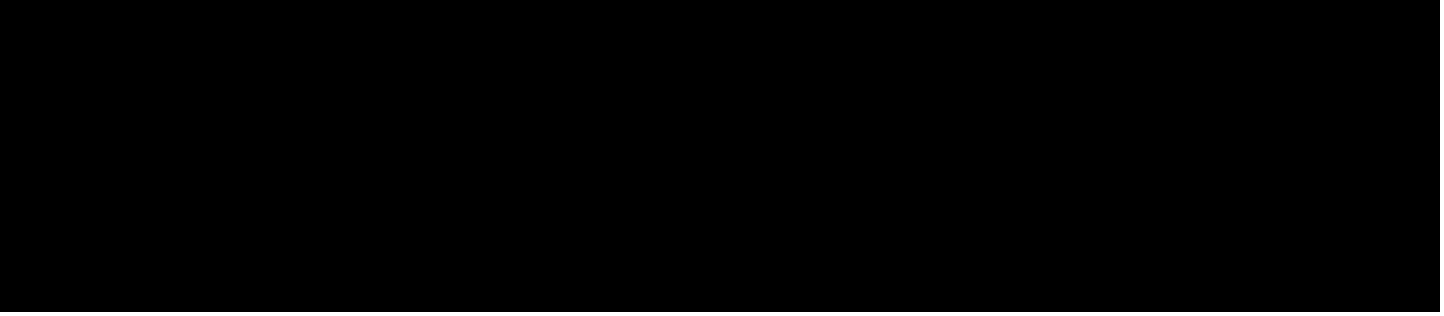
Developer further agrees it will not integrate the Software into any Application or Beta Application (i) with end users who Developer has actual knowledge are under the age of 13, or (ii) that may be deemed to be a "Web site or online service directed to children" as defined under the Children's Online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

19% share identifiers or personal information with **SDKs not allowed in children's apps**

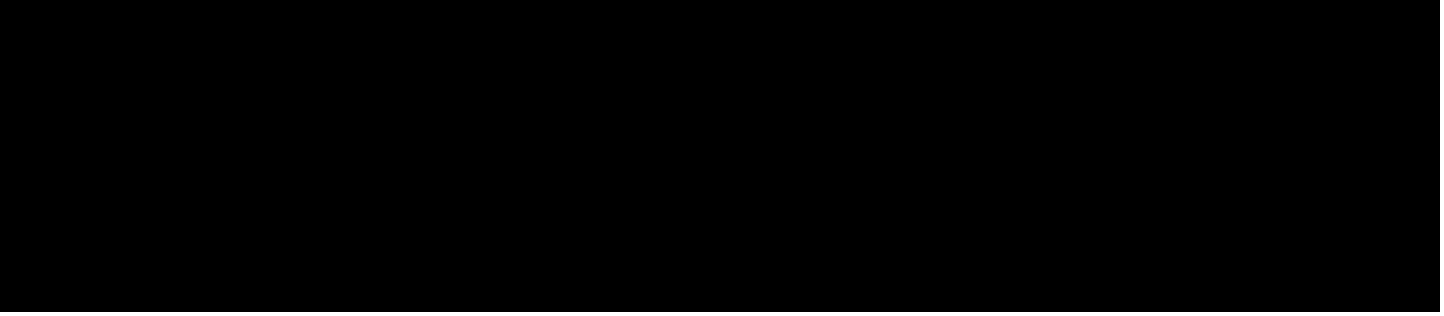
SDK	TOTAL DFF INSTALLS
crashlytics	556M
supersonic + ironSource	481M
Tapjoy	386M
mopub	296M
INNERACTIVE	239M
heyZap	150M

40% share identifiers and personal info
without using encrypted HTTP

data sharing obfuscation



```
"locations":"TCsxMiMiMyhfKTInOjYmK0E8Ii..."
```



```
"locations":"TCsxMiMiMyhfKTInOjYmK0E8Ii..."
```

```
L+12#"3(_)2':6&+A<"*.80#W47*!"08E%7.
```

```
"locations":"TCsxMiMiMyhfKTInOjYmK0E8Ii..."

        L+12#"3(_)2':6&+A<"*.80#W47*!"08E%7.
XOR     ENCRYPTIONKEYENCRYPTIONKEYENCRYPTION
XOR     $T@RT@PP$T@RT@PP$T@RT@PP$T@RT@PP$T@R
        ------------------------------------

        -122.27143907388712,37.8692660985882
```

```
const-string v0, "f188c2f6176602368ab346d0b40f1098ed350c3c46595e9981a8db1db9d865b7"

invoke-static {v0}, Lcom/revmob/internal/l;->c(Ljava/lang/String;)[B

move-result-object v0

const-string v1, "3066546c3043314e614c4b764f433338"

invoke-static {v1}, Lcom/revmob/internal/l;->c(Ljava/lang/String;)[B

move-result-object v1

new-instance v2, Ljavax/crypto/spec/SecretKeySpec;

const-string v3, "AES/CBC/PKCS5Padding"

invoke-direct {v2, v0, v3}, Ljavax/crypto/spec/SecretKeySpec;-><init>([BLjava/lang/String;)V

const/4 v0, 0x0

:try_start_0
const-string v3, "AES/CBC/PKCS5Padding"

invoke-static {v3}, Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

move-result-object v3
```

```
GET /api/v1/21a5e0d7210e450e94753eadf2dd5571/apa/
?ts=1497147282
&s=8286782666719854066
&su=104445ca47ea5bcfee9ed26f244180d7,
    353627079437060,
    0dc37ed8f864910b942c4830762cd947,
    0dc37ed8f864910b942c4830762cd947,
    1368c15e70a6326602dea67b355953beb0634d78,
    1368c15e70a6326602dea67b355953beb0634d78,
    188062b1844b1369691259313cdd026260c9a7481e065cdd01432a77c423c23f,
    188062b1844b1369691259313cdd026260c9a7481e065cdd01432a77c423c23f,
    b07adb5ec8d1818c,
    ca1bb70e447538018ebca1e24b1eed55,
    a6ab201d7f9925973a841b80a61638b7,
    8493cd4071646070163ac8eba574247009eaadc3,
    a723a5f5126c983acb34bd4d41497c7d73d46d3c,
    ba93bc93263c9a48d3c73a1c60984554d7462e239cc9d54c24de97257e4660d5,
    dee70dd93a1d4152fb7cb846dc08ab2688932254037be8b40b1e007caeab9fa8
&imei=353627079437060
&bid=com.mattel.ghouls
&aid=b07adb5ec8d1818c
&kt_v=au1.4.3
TTP/1.1
Host: api.geo.kontagent.net
Connection: Keep-Alive
User-Agent: android-async-http/1.3.1 (http://loopj.com/android-async-http)
Accept-Encoding: gzip
```

```
GET /api/v1/21a5e0d7210e450e94753eadf2dd5571/apa/
?ts=1497147282
&s=8286782666719854066
&su=104445ca47ea5bcfee9ed26f244180d7,
    353627079437060,                          IMEI
    0dc37ed8f864910b942c4830762cd947,         MD5(IMEI)
    0dc37ed8f864910b942c4830762cd947,
    1368c15e70a6326602dea67b355953beb0634d78,
    1368c15e70a6326602dea67b355953beb0634d78,  SHA1(IMEI)
    188062b1844b1369691259313cdd026260c9a7481e065cdd01432a77c423c23f,   SHA256(IMEI)
    188062b1844b1369691259313cdd026260c9a7481e065cdd01432a77c423c23f,
    b07adb5ec8d1818c,                         Android ID
    ca1bb70e447538018ebca1e24b1eed55,         MD5(b07adb5ec8d1818c)
    a6ab201d7f9925973a841b80a61638b7,         MD5(B07ADB5EC8D1818C)
    8493cd4071646070163ac8eba574247009eaadc3, SHA1(...)
    a723a5f5126c983acb34bd4d41497c7d73d46d3c,
    ba93bc93263c9a48d3c73a1c60984554d7462e239cc9d54c24de97257e4660d5,      SHA256(...)
    dee70dd93a1d4152fb7cb846dc08ab2688932254037be8b40b1e007caeab9fa8
&imei=353627079437060
&bid=com.mattel.ghouls
&aid=b07adb5ec8d1818c
&kt_v=au1.4.3
TTP/1.1
Host: api.geo.kontagent.net
Connection: Keep-Alive
User-Agent: android-async-http/1.3.1 (http://loopj.com/android-async-http)
Accept-Encoding: gzip
```




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


ESRB
PRIVO®
Privacy & Permission=TRUST
kidSAFE®
SEAL PROGRAM
TrustArc
the new TRUSTe
INTEGRITY
Children's Advertising Review Unit®
iKeepSafe

The Switch

Thousands of apps in Google Play Store may be illegally tracking children, study finds

(Matt Rourke/AP)

By Hamza Shaban April 18 Email the author

The Washington Post

Democracy Dies in Darkness

Fun Kid Racing

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

Everyone

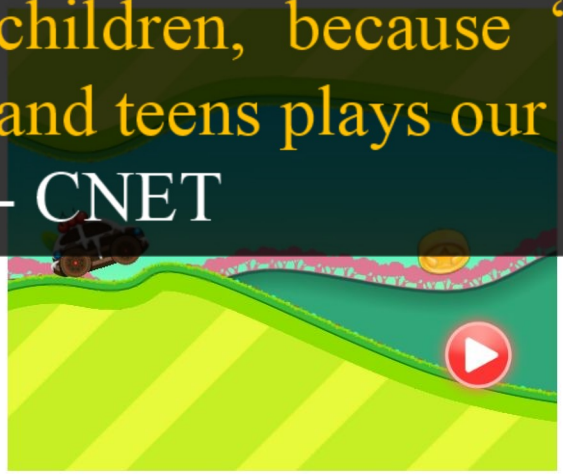
Contains Ads · Offers in-app purchases

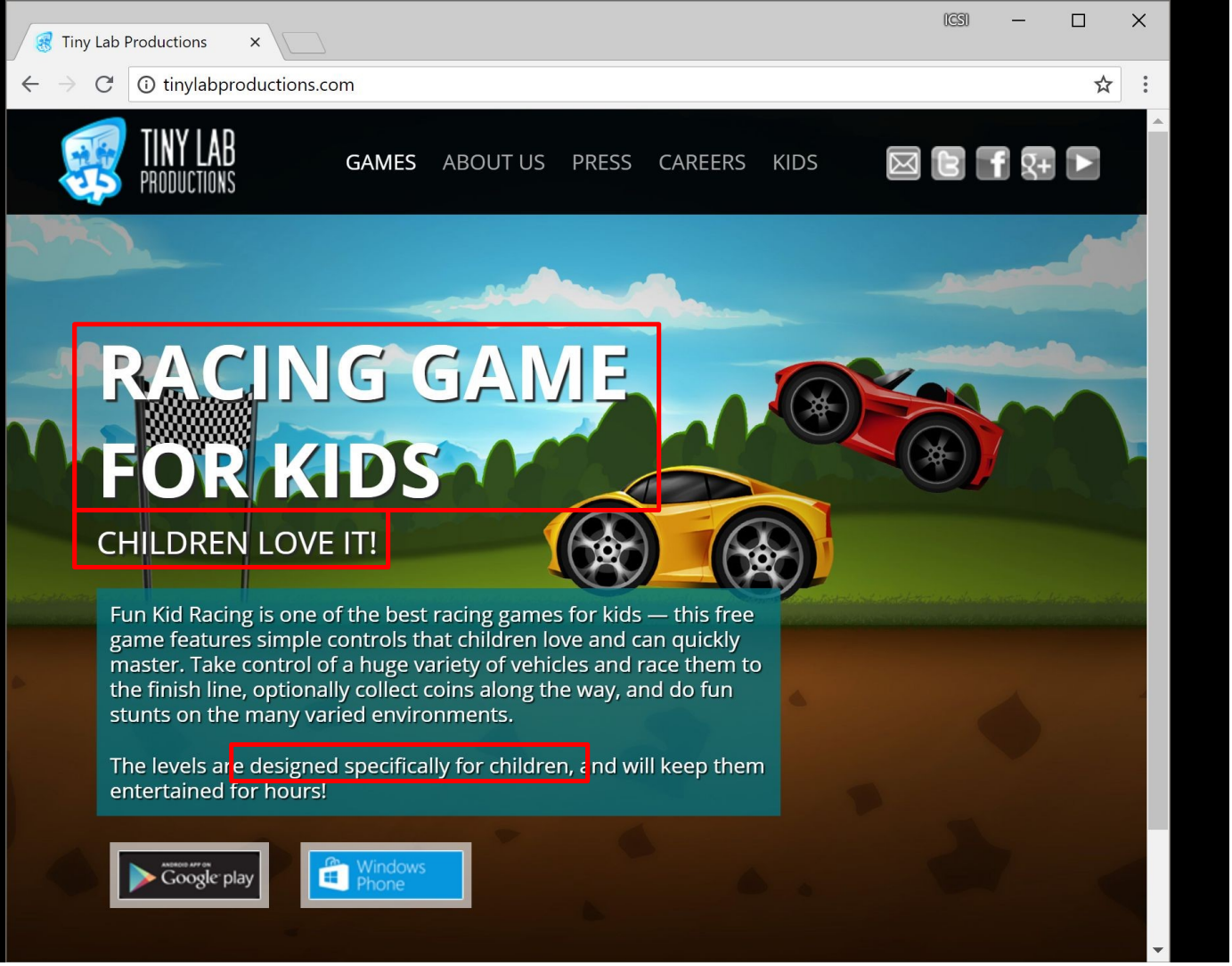
You don't have any devices

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




Tiny Lab Productions
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

Mixed Audience Apps ("Not Primarily" directed to children)

5

under 13

Sources: Magic Circus Festival, Funny Animal Dance, Dino Tim
***As of 4/20/2018**

"Shapes, colors, counting games, numbers, basic skills… With "Dino Tim" kids in preschool age (***3, 4, 5 and 6 years old***), **primary school and kindergarten** will learn with no effort while having fun.) It suits perfectly to every age although **it's specifically suggested for kindergarten, preschool and primary school (3-8 years)** and adults of all ages."

Source: https://play.google.com/store/apps/details?id=com.EducaGames.DinoTim

closing recommendations

developers: use compliant SDKs and options

SDK providers: enforce terms of use

platform providers: stricter security and analysis

users: privacy awareness

We need more privacy auditors

https://appcensus.mobi

https://blog.appcensus.mobi

https://www.petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf