

“is our children’s apps learning?”

automatically detecting COPPA violations



Irwin Reyes

Primal Wijesekera

Abbas Razaghpanah

Joel Reardon

Narseo Vallina-Rodriguez

Serge Egelman

Christian Kreibich

My name is Irwin Reyes from the International Computer Science Institute. I'll be speaking to you about our ongoing work to automatically identify privacy issues in mobile apps for kids.

data from children

the children's online privacy protection act (COPPA)
limits data collection from children under 13

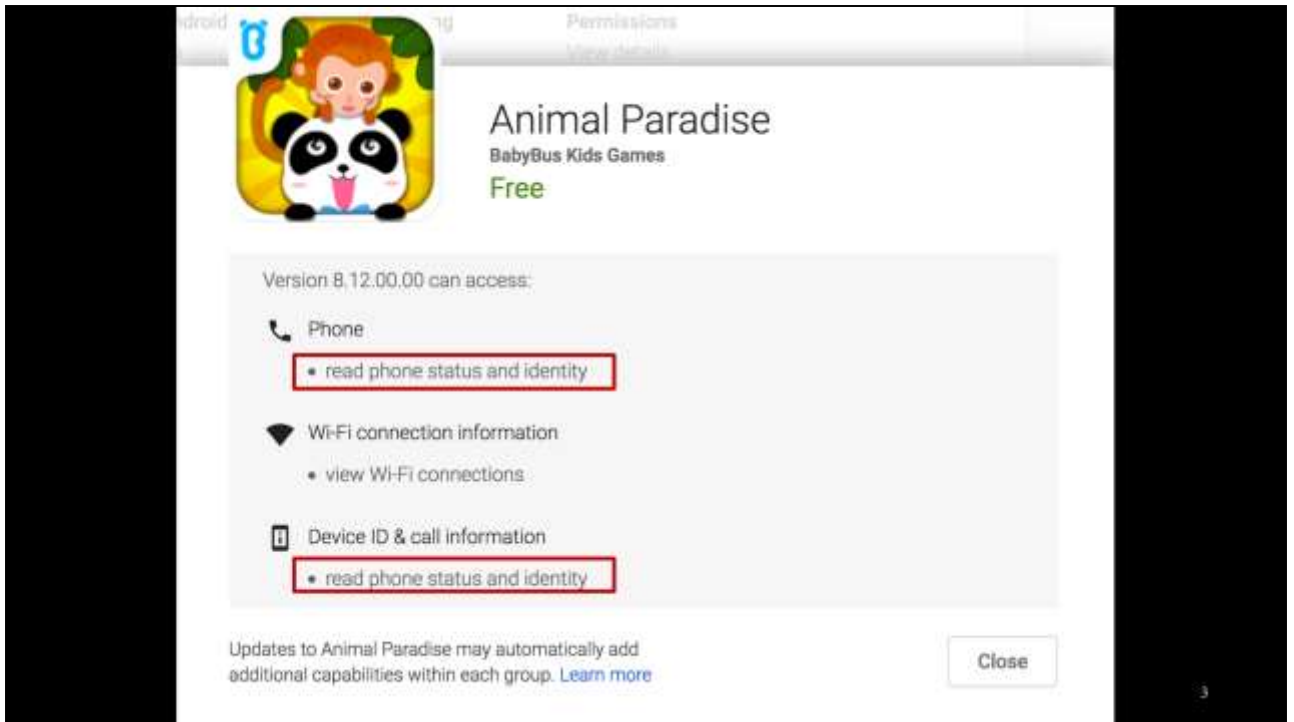
- contact information (e.g., email, phone number)
 - audio / photo / video
 - physical address / geolocation
 - persistent identifiers
-
- must obtain parental consent

First, a bit of background. In the United States, we have the Children's Online Privacy Protection Act – COPPA, for short. COPPA governs how online services such as mobile apps collect data from users under 13 years of age.

This regulation limits the gathering personal information like email addresses and phone numbers, audio/visual captures, and the fine geographic location of children.

Additionally, COPPA restricts the collection and use of persistent identifiers that can be used to uniquely identify individuals over time and across different services. Persistent identifiers include hardware serial numbers and software fingerprints. Using these for behavioral advertising is prohibited.

In cases where a mobile app operator wishes to collect restricted data for internal operational purposes (e.g., infrastructure maintenance, high score lists), they must notify parents of this and obtain parental consent prior to collection.



Let's step through an example of how notice and consent is done. Here, the developer BabyBus declares that their Animal Paradise game is able to access device identifiers. Note that these declarations just mean the app *can* use those privileges, not that they actually do so. Still, parents can review this list prior to installing an app and decide if this is appropriate.

PRIVACY POLICY

This Privacy Policy ("Policy") provides important information regarding BabyBus (Fujian) Network Technology Co., Ltd ("BabyBus," "we," or "our") in respect to user information collected through our mobile applications and the use of the information. You provide consent to this Policy when your access and use BabyBus applications ("Products") and other related services ("Services").

- 1. Personal and non-personal information.

We understand the importance of our users' personal information, and more importantly the information pertaining to children under 13 years of age. We do not collect or require users to enter their personal information when using our Products. We do not collect any personal information from children with our Products.

When using our Products, we might read non-personal information (such as internet, Wi-Fi availability, network connection, wake lock, device status, internal and external storage availability and usability) for the use of Product development and Service improvement. The collection of information will be used for the development and functional improvement of our Products to ensure quality user experience. We only collect such information to the extent that allow us to conduct our normal business operation and Products' research and development.

Any information we received will be used internally for the purpose of product development and to third parties performing services on our behalf, who comply with our Privacy Policy. We will not disclose your information publicly unless we have received your consent or under government order.

- 2. COPPA

We comply with the Children's Online Privacy Protection Act. We do not knowingly collect personal information on children under the age of 13. When a user identifies himself or herself as a child under the age of 13 through a support request or through any feedback, we will not collect, store or use, and will delete in a secure manner, any personal information of such user.

Developers also provide privacy policies to further elaborate on their data collection practices. In BabyBus's privacy policy, the developer states that any data collection is strictly for product maintenance purposes.

- 5. Third party websites and links.

We may provide links to our website or third party websites. Our Privacy Policy will have no effect on any third party websites' privacy policy or their usage of personal information collected. Our Privacy Policy as expressed herein does not apply to other parties, and we do not dictate the collection or usage of information by them. We do not take part in the operation of third party advertisers or websites. Please find the list of third party companies below:

Umeng

TalkingData

AdsMOGO

AdMob

InMobi

Baidu

Tencent

5

However, disclosures don't always tell the full story. Further down in the privacy policy for the Baby Panda Care game, the developer lists third-party websites that the developer might link to, and that this policy does not apply to them.

They fail to mention a number of important details:

- First, although the policy doesn't explain how these are integrated into products, if at all
- Second, that a number of these are not just websites, but advertising libraries that may be bundled with apps to target apps to particular users
- And finally, that one of those advertisers, InMobi...



Home » News & Events » Press Releases » Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without 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

FOR RELEASE

June 22, 2016

TAGS: Children's Online Privacy Protection Act (COPPA) | Technology | Mobile |

Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Children's Privacy | Consumer Privacy

Singapore-based mobile advertising company InMobi will pay \$950,000 in civil penalties and implement a comprehensive privacy program to settle Federal Trade Commission charges it deceptively tracked the locations of hundreds of millions of consumers – including children – without their knowledge or consent to serve them geo-targeted advertising.

6

last year settled with the FTC for the silent collection of sensitive geolocation data from children.

disclosures list what apps might do

At best, disclosures list what apps might do: they might access a piece of identifying information, or might share it with this third-party company or that.

let's find out what apps **actually do**

8

What we want is something more actionable. Let's find out what apps actually do.

custom android for logging api calls



lumen app for network flow analysis



P. Wijesekera, A. Backar, 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

N. Vallina-Rodriguez, S. Sundaresan, A. Razaghpanah, R. Nithyanand, M. Allman, C. Kreibich, P. Gill, *Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem*, Data and Algorithmic Transparency Workshop (DAT) 2016

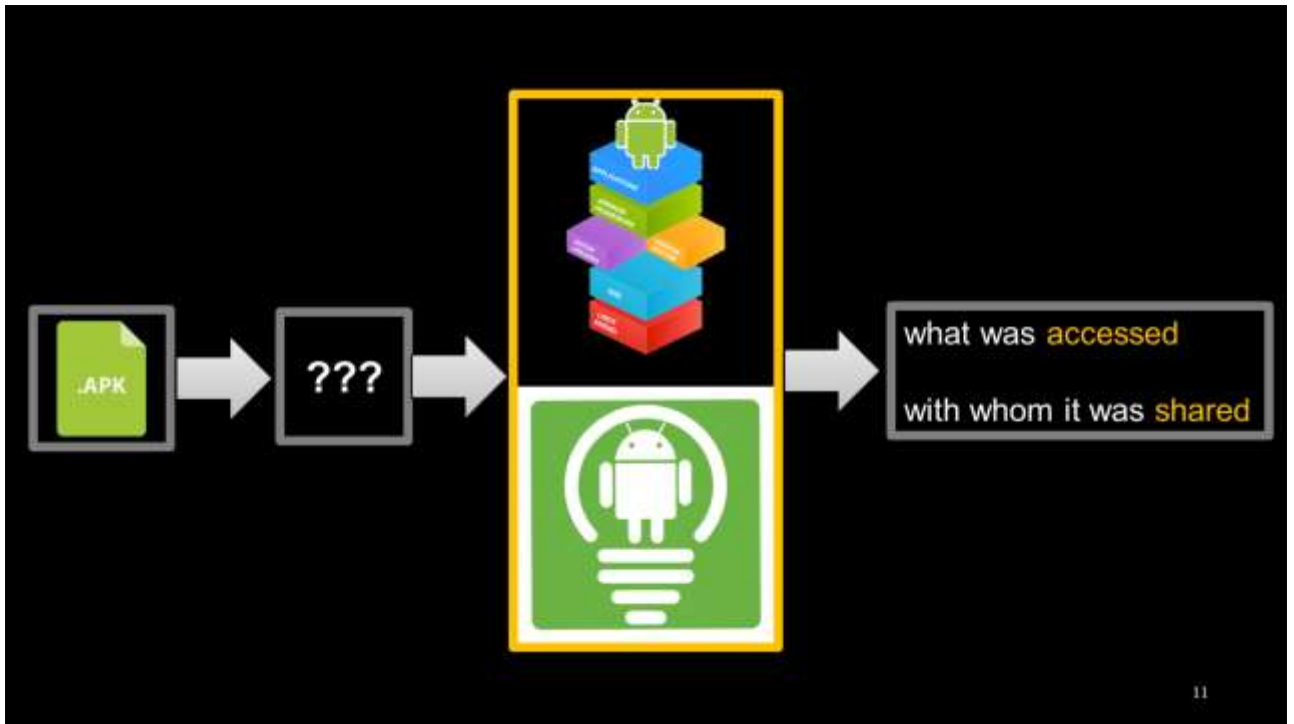
9

To that end, we propose a method of dynamic analysis to characterize how apps access and share sensitive data. We combine two of our existing tools: First, an instrumented version of the Android platform to determine which sensitive API calls are being invoked. This is part of the work on permission systems my colleague Primal Wijesekera presented in yesterday's session. And second, the Lumen network flow tool to examine what data is leaving the device and to whom it's going, even over TLS-protected communications.

we evaluate apps **without modifying them**

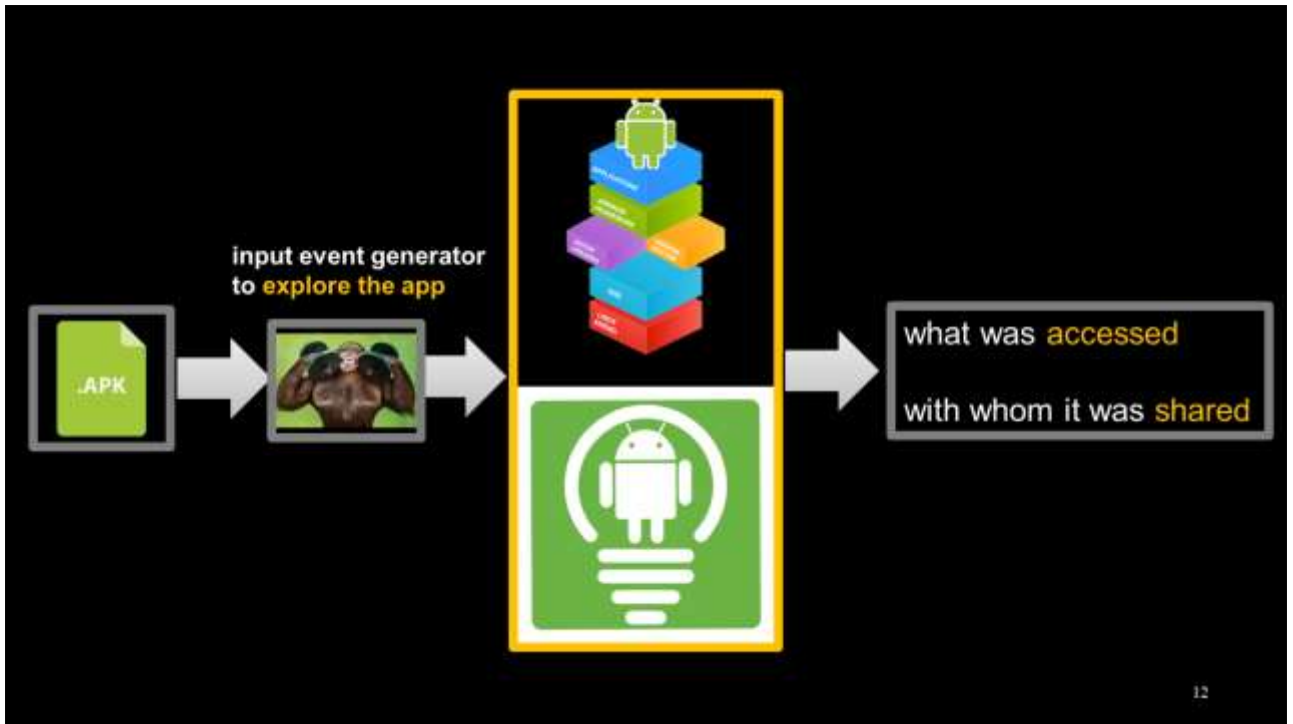
10

This dynamic analysis approach allows us to examine apps without having to modify them or otherwise examine their internals. We can download apps and run them as-is, exactly how a consumer would use them.



Dynamic analysis does present a technical challenge, in that it's insufficient to just run the application on a testbed with our tools.

We need someone or something to actually interact with the app being tested. Otherwise, we would only observe the app's behavior as it sits on its initial screen. We'd like to be able to examine apps at scale.

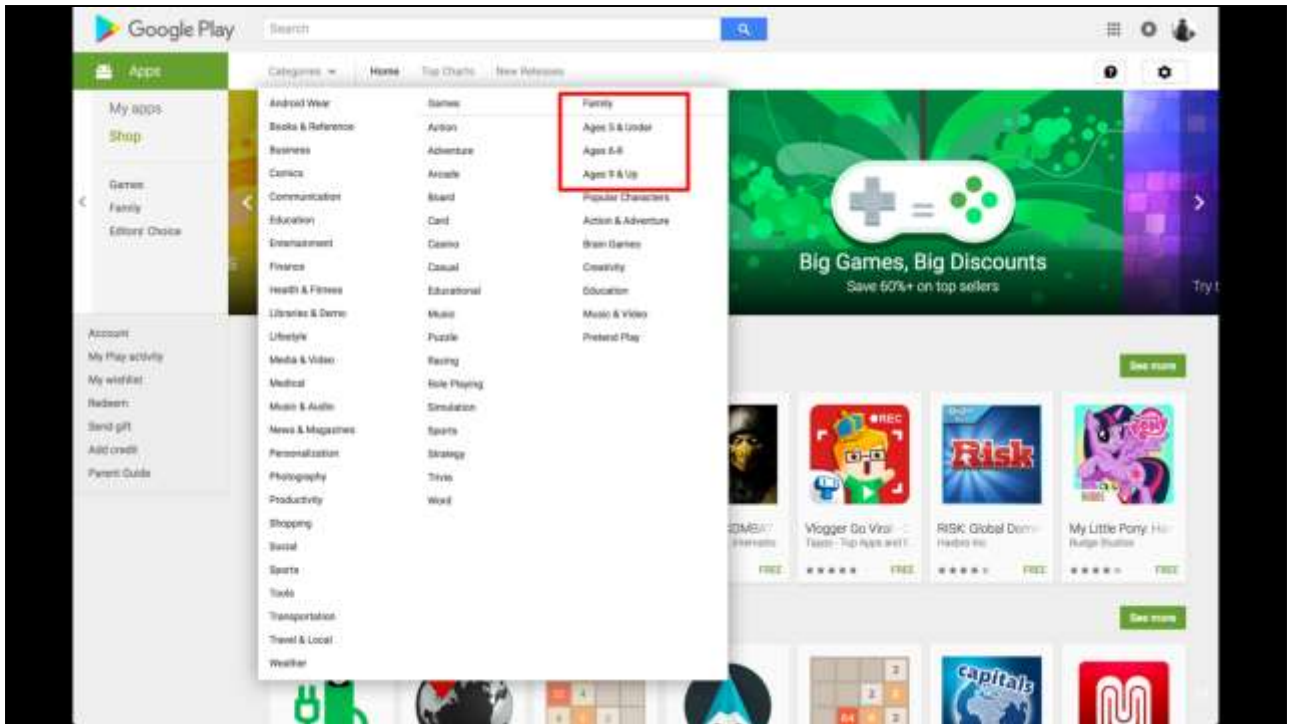


For that, we turn to the Android Exerciser Monkey, a tool included in the Android SDK that generates a pseudorandom stream of input events – taps, swipes, and screen transitions. In our internal testing, we found that Monkey had comparable coverage to that of an undergraduate tester in a majority of the children’s apps evaluated – no surprise, given the simple nature of apps meant for toddlers and young children.

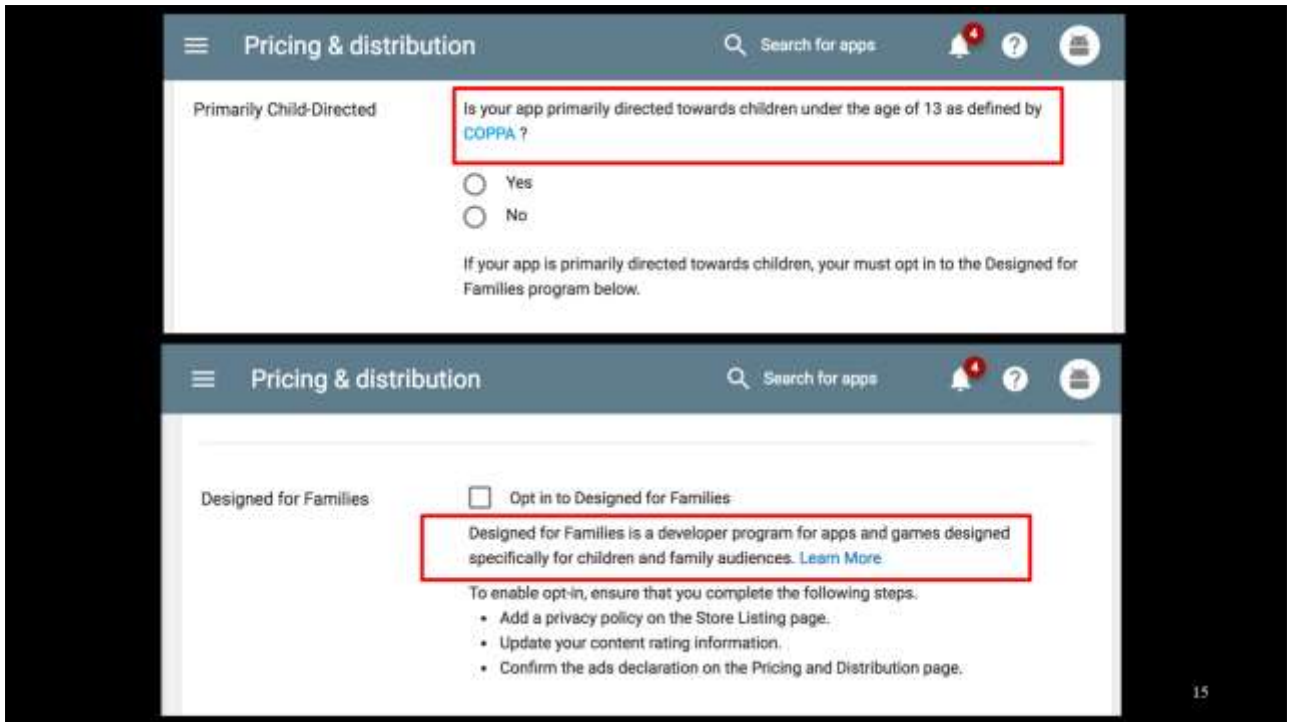
what we **found**

13

This system has been built and been used to test a number of children's apps.



We collected free apps from the Google Play Store listed under child-specific categories.



Developers who list their apps in those child-specific categories must opt-in to Google Play Store

a corpus of **735** children's apps

initial **167** downloaded november 2016

additional **568** downloaded april 2017

16

All in all, we built a corpus of 735 free apps explicitly targeted to kids.

This was done in two stages as we developed our test pipeline.

out of 735 apps tested

- 41% share at least one type of persistent hardware identifiers with third-parties
 - 36% hardware serial number
 - 13% imei
 - 8% wi-fi mac address

Innovations

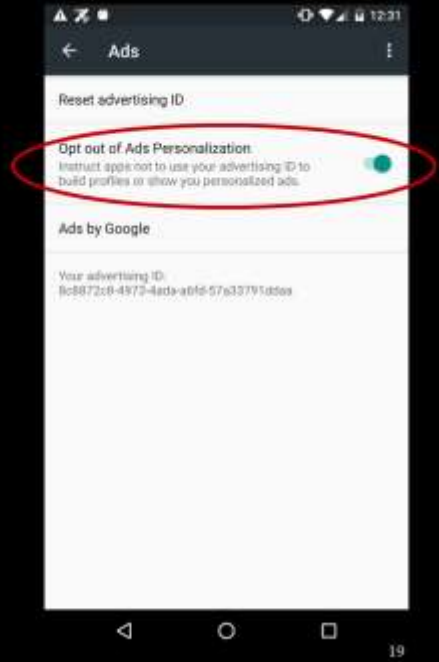
Uber's 'fingerprinting' of iPhones after users delete app has sparked an FTC complaint

By Steven Overly April 27



out of 735 apps tested

- 51% share the google advertising identifier despite having opted out
- ideal behavior: don't share at all, or send non-unique fixed value



out of 735 apps tested

- 29 apps use device geolocation functionality
- 6 transmit geolocation data to third-parties
- 3 do so using unencrypted HTTP

- 5 apps read the registered google account
- 3 transmit the email address to third parties
- all use TLS

AppCensus

basketball

- [Basketball](#)
- [Basketball](#) Football Teams
- [Basketball](#) HD Wallpapers
- [Basketball](#) Learning
- [Basketball](#) Live for EuroLeague
- [Basketball](#) Sniper
- [Basketball](#) Training Workout
- [Best Basketball](#) Shot
- [Big Finger Basketball](#)
- [Double Basketball](#) Free
- [Flying Basketball](#) Slam Dunks
- [Guest for Basketball](#) Player

By Category ▾

About

Contact

Personal Information

We searched for the following data types:

-  Location
-  Phone
-  Email



Location

Device Identifiers

We searched for the following data types:

-  IMEI
-  Wi-Fi Mac
-  AAID



AAID



Hardware Identifiers

Multimedia

We searched for the following data types:

-  Photo
-  Video
- 

No personal data detected leaving the device during our testing.

what's next

- virtualized testbed: **scalable tests** on commodity servers
- **crowdsourcing** to help “stranded” monkeys
- expanded analysis to **all apps**
- **trends** over time

THANK YOU!