

March 31, 2021

Re: Request to Investigate Google’s Unfair and Deceptive
Practices in Marketing Apps for Children

Dear Acting Chair Slaughter and Commissioners Chopra, Phillips, and Wilson:

Campaign for a Commercial-Free Childhood (CCFC) and the Center for Digital Democracy (CDD) write to update and renew their request, filed December 19, 2018, that the FTC investigate whether the Google Play Store is violating Section 5 of the Federal Trade Commission Act by representing that children’s apps on its platform are safe and appropriate for children when they are not.¹ The FTC’s failure to take earlier action has permitted Google Play to continue promoting apps for children that are not safe or appropriate because they do not comply with the COPPA Rule.² Stopping Google Play’s misrepresentations is even more critical today because children are spending even more time on mobile devices using apps due to the COVID-19 pandemic.

I. Google has changed how it treats apps intended for children, but has not fixed the problem that many children’s apps are not complying with COPPA

Our 2018 Request showed that many apps in the Family section of Google Play, including some apps displaying the family-friendly star and/or listing specific age ranges under age 13, were not complying with the COPPA Rule.³ Since that time, Google Play has changed the criteria for inclusion in the Designed for Families program. It has also created a process of awarding a “Teacher approved” badge to certain apps. As a result of these changes, any app declaring a target audience that includes children under the age 13 must comply with Google Play’s Designed for Family policy. Some of these apps undergo an additional review process and can be designated as “Teacher approved.” The Teacher approved badge seems to have replaced the family-friendly star described in the 2018 Request. Currently, all apps listed in the

¹ Request to Investigate Google’s Unfair and Deceptive Practices in Marketing Apps for Children (Dec. 19, 2018)(“2018 Request”), available at <https://bit.ly/2018Request>.

² 16 CFR §312, *et. seq.*

³ 2018 Request at 11-28.

Google Play Store as Kids apps have the “Teacher approved badge.” The Play Store continues, however, to offer many other apps that target children that do not have the Teacher approved badge.⁴

A. Changes to the Designed for Families program

Google Play updated its Designed for Families program and related Families Policy on May 29, 2019.⁵ Under the revised policy, all developers must declare their target audience(s) from the following options: ages 5 and under, 6-8, 9-12, 13-15, 16-17, and 18 and over.⁶ Both apps that target children under 13 and those that target children and older users must comply with Google’s Families Policy.⁷

The Families Policy includes requirements such as:

- Make sure that any content in your app that could be seen by children is appropriate for them.
- Display only ads that are appropriate for children, and use ad SDKs from the Families Ads Program.
- Make sure your app (including all APIs, SDKs, and ads) complies with all applicable laws and regulations relating to children, including the US Children's Online Privacy Protection Act (COPPA), and the EU General Data Protection Regulation (GDPR).⁸

Finally, apps whose target audience only includes children must follow additional requirements in the Designed for Families program.⁹ The Designed for Families program requires that apps use only Google Play certified software development kits (SDKs).¹⁰

⁴ See Ex. B for an example of how parents would find each type of app.

⁵ *Creating Apps and Games for Children and Families*, <https://developer.android.com/google-play/guides/families>. The earlier criteria are described in the 2018 Request at 12-14.

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.* Apps that targets both children and older audiences are not required to also participate in the Designed for Families program, but may choose to do so if they meet the requirements.

¹⁰ *Participate in the Families Ads Program*, <https://support.google.com/googleplay/android-developer/answer/9283445>.

B. Teacher approved apps

Google Play launched Teacher approved apps in April 2020 in response to COVID-19. A blog by the Google Play Product and UX Director, Kids and Families explained:

We've heard from parents that it's difficult to dig through all the content that's out there for kids. Today, we're making it easier for parents to find the good stuff, with a new Kids tab on Google Play filled with "Teacher approved" apps that are both enriching and entertaining. We decided to launch the Kids tab a bit earlier than planned because parents who have tried it out told us that it's been helpful, especially now with their kids home from school and spending more time with screens.¹¹

The blog explains that "[a]pps rated by teachers that also meet Google Play's quality standards receive a 'Teacher approved' badge." The blog advises that "Whenever parents search the Play Store, they can look for the 'Teacher approved' badge to quickly see which apps have been reviewed and rated highly by teachers."¹²

The Parent Guide to Google Play provides the same advice. It tells parents to open the Google Play Store and tap on "Kids" at the top. It states that all apps in the Kids section are Teacher approved.¹³ The Parent Guide also informs parents that the "Teacher approved" badge means:

Google consulted with academic experts to develop a framework for rating apps, and then worked with teachers and specialists across the US to rate them based on our framework.

Teacher approved apps are:

- Age appropriate
- Thoughtfully designed
- Fun or inspiring

Teachers and specialists only rate apps for the age groups that they teach and they have all been vetted, trained, and evaluated before they become part of the program.¹⁴

¹¹ Mindy Brooks, *Find high-quality apps for kids on Google Play*, (April 15, 2020), <https://blog.google/products/google-play/teacher-approved-apps/>. This blog can also be found by clicking on "Learn more about the Teacher approved badge" in the Parent Guide to Google Play. A copy of the blog is included as Ex. A.

¹² *Id.*

¹³ The Parent Guide is available online, at <https://support.google.com/googleplay/answer/6209547?hl=en>, and on the Google Play Store. A copy is included as Ex. C.

¹⁴ Parent Guide.

Only apps that participate in Google’s Designed for Families program may be considered for a Teacher approved badge.¹⁵

II. Google’s representations to parents are misleading

Although Google’s representations have changed since the 2018 Request was filed, it still represents that all apps on the Play Store intended for children under age 13, even as part of the audience, must be appropriate for children and comply with COPPA. It further represents that the Teacher approved apps not only are appropriate and comply with COPPA, but are high-quality and beneficial for children.

These representations are misleading because many apps directed to children may not be complying with COPPA. The COPPA Rule prohibits the collection, use and sharing of persistent identifiers used to profile children or serve targeted advertising to them in the absence of notice to parents and advance verifiable parental consent. The 2018 Request cited, as evidence that children’s apps on the Play Store were not COPPA-compliant, a study finding that roughly 57% of the 5,855 child-directed apps on the Google Play Store were transmitting children’s personal information to third parties without giving notice or obtaining consent.¹⁶ Since the 2018 Request was filed, three new studies have found that a significant number of children’s apps were collecting and sharing children’s personal information without complying with the COPPA Rule. Additional evidence of widespread non-compliance with COPPA by children’s apps comes from three related class actions brought by parents over gaming apps for kids.

A. Recent studies suggest that many apps intended for children are still not complying with COPPA.

A study published in *JAMA Pediatrics* in September 2020, *Data Collection Practices of Mobile Applications Play by Preschool-Aged Children*, tested 451 apps used by children aged five and under, 153 of which were in the Google Play Store’s family section.¹⁷ The data was collected between August 2018 and January 2020.¹⁸ The study found that 67% of the apps tested showed transmission of identifiers to third-party domains.¹⁹ The “most commonly transmitted identifier was the advertising identifier, which is used to create advertising behavioral profiles of

¹⁵ *Participate in the Families Ads Program*, <https://support.google.com/googleplay/android-developer/answer/9283445>.

¹⁶ 2018 Request at 8-9 and 23, citing Irwin Reyes, *et al.*, *Won’t Somebody Think of the Children?*” *Examining COPPA Compliance at Scale*, Proceedings on Privacy Enhancing Technologies: 2018 (3) 63-83 (“*PET Study*”). The Request at 9 also identified a May 2018 Oxford study finding that children’s apps had the largest number of third-party trackers.

¹⁷ Fangwei Zhao, *et al.*, *Data Collection Practices of Mobile Applications Played by Preschool-Aged Children*, *JAMA Pediatrics*, 2020;174(12) at 4 (published online Sept. 8, 2020)(“*Pediatrics Study*”).

¹⁸ *Id.* at 1.

¹⁹ *Id.* at 4.

users.”²⁰ The study also found that children being raised by parents without advanced degrees showed two to three times higher rates of data transmission to third parties.²¹

Looking only at the 153 apps included in Google Play’s Designed for Families category, the study found that 46% transmitted advertising identifiers.²² While this percentage is lower than the overall finding, it is still remarkably high. Moreover, the study also found that 44% of apps in the Designed for Families category had zero transmissions.²³ This finding suggests that apps do not need to transmit advertising identifiers in order to function.²⁴

The *Pediatrics Study* concluded that

the collection and sharing of children’s data are highly prevalent, and disparities exist by parent education. These results highlight the need for comprehensive testing of app and platform data collection practices by regulatory bodies so that updated privacy legislation can be crafted that adequately children’s rights in the modern digital environment.²⁵

The second study was conducted by researchers at the International Digital Accountability Council (IDAC), an offshoot of the industry-supported Future of Privacy Forum.²⁶ They tested over 500 of the top educational apps in the Google Play Store in July 2020.²⁷ They found five problems that likely violate COPPA (assuming the app is child-directed or the operator has actual knowledge the user is a child). They are:

(1) sharing location data and persistent identifiers with third-parties;

²⁰ *Id.* at 6. The most common identifier was the Android advertising IDs (AAID) with 2283 transmissions. The AAID used to create advertising behavioral profiles of users. Other persistent identifiers included the Android identifier (824 transmissions), hardware ID (37), geolocation (30), user’s phone number (10) and users real name (5). *Id.* at 4. On average, each app transmitted three identifiers, with a maximum of 57. *Id.* The study notes that while the advertising identifier is technically resettable, few parents are likely to have the technical knowledge to do so. *Id.* at 6.

²¹ *Id.* at 6.

²² *Id.* at 4.

²³ *Id.*

²⁴ Indeed, the *Pediatrics Study* notes that the types of persistent identifiers that track users across apps are not needed for the types of analytics that help apps function better. *Id.* at 6.

²⁵ *Id.* at 7.

²⁶ IDAC, About Us, <https://digitalwatchdog.org/about/>.

²⁷ Quentin Palfrey, et al., *Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic*, International Digital Accountability Council, at 2 (Sept. 1, 2020)(“*IDAC Study*”). The researchers manually tested 78 apps and automatically tested 431.

- (2) exposing personal data in their URLs, raising security concerns;
- (3) allowing a large number of third-parties to collect user information;
- (4) engaging in ID-bridging, a practice that allows apps to circumvent users' privacy controls; and
- (5) embedding potentially invasive and unnecessary software development kits (SDKs).²⁸

Of particular relevance, the investigation revealed that numerous apps were transmitting personal data, including IMEIs, and Android IDs used for behavioral advertising, to third-parties.²⁹ The third-parties receiving the most data from the apps were Facebook, Unity, AppsFlyer, Mixpanel, Branch.io, OneSignal, MoPub, Applovin and Flurry.³⁰

The researchers found that “[s]ome analytics and advertising third-parties appear to be quite aggressive with respect to their data-collection practices in the ed tech context. Moreover, it appears that in some cases developers may not be aware of the data collection that is occurring.”³¹ They also observed that allowing third-parties to offer marketing, analytics, or advertising services went against the best practices in the Future of Privacy Forum’s Student Privacy Pledge.³²

The *IDAC Study* found the practice of ID-bridging to be both widespread and troubling.³³ This term refers to the practice of using a persistent identifier (either an Android ID or AAID) to continue to identify a user, even after the user resets one of the IDs. This practice violates Google policy, which prohibits developers from sharing both the Android ID and the AAID to prevent third parties from tracking users based on historical data after the user has reset the advertising ID.³⁴ Nonetheless, the IDAC researchers observed that 15 of the 78 apps tested manually and 203 of 421 apps tested automatically were collecting and sharing *both* the Android ID and the AAID together.³⁵

The *IDAC Study* concluded that “mobile analytics and advertising SDKs pose particular risks in ed tech apps -- especially apps that have younger users -- because of their monetization

²⁸ *Id.* at 1.

²⁹ *Id.* at 9. IMEIs and Android IDs are used to target advertising. Other personal information included names, emails, location, username, passwords, and age. *Id.*

³⁰ *Id.* at 11.

³¹ *Id.* at 10.

³² *Id.* at 11.

³³ *Id.* at 11-14

³⁴ *Id.* at 12.

³⁵ Researchers also found that 223 third-parties received both the Android ID and the AAID. *Id.* at 13. The third parties receiving both identifiers most often included Facebook, DoubleClick, MoPub, Appsflyer. *Id.* at 13.

capabilities.”³⁶ It found that “20 of the 78 Android manually-tested apps in our investigation revealed the presence of analytics or advertising third-party SDKs. These types of SDKs should rarely be used in children’s ed tech apps because of the potential for these SDKs to covertly collect personal information, including location and persistent identifiers.”³⁷

The third study finding the transmission of children’s personal information to third parties without parental notice and consent was conducted by AppCensus for the Australian Competition and Consumer Commission. AppCensus analyzed 1,000 of the most popular mobile Android apps in Australia in June and July 2020.³⁸ The sample included 100 Kids Apps. It found that 47% of Kids apps transmitted the Android Advertising ID (AAID) and 46% transmitted the Android ID.³⁹ The three most common companies contacted by Kids apps during the testing period were Google (34%), Unity Technologies (29%) and Facebook (13%).⁴⁰

Our observations made in preparing this filing also indicate that child-directed apps on Google Play are continuing to transmit personal information to third parties without obtaining parental consent. Ex. D shows the AppCensus analysis of the two examples of child-directed apps in Ex. B -- Hatchimals COLLEGGtibles and Bubbu - My Virtual Pet. At the time of testing, both transmitted sensitive data to third parties.⁴¹ The “Teacher approved” app Hatchimals COLLEGGtibles transmitted three device identifiers -- Advertising ID, Android ID and Device Description. During the testing period, it made four transmissions to Unity and one to Swrve. Transmitting both the Advertising ID and Android ID to Unity appears to violate Google’s policy against ID-bridging. Swrve is not on the list of Google certified SDKs. Its goal is to “help customers know every user, anticipate their needs, and interact in the right moment, with the right message in the right channel.”⁴² The other app, Bubbu - My Virtual Pet, transmitted the Advertising ID to Unity (2 times) and once to Kidoz, and transmitted a Device Description to Crashlytics during the testing period.

Thus, all three studies as well as our own research indicate that widespread COPPA Rule violations are still occurring on child-directed apps on Google Play.⁴³ Despite the large number of non-compliant children’s apps, however, to our knowledge, Google has only removed three children’s apps from the Play Store for violating its data collection policies, and that occurred

³⁶ *Id.* at 15.

³⁷ *Id.*

³⁸ AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, Sept. 24, 2020, <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/accc-commissioned-research>.

³⁹ *Id.* at ii, Fig. 1 and App. C, Table 31. Email, GPS location, and name were each transmitted by 2% of Kids apps.

⁴⁰ *Id.* at App. C, Table 33 (which lists the top 10).

⁴¹ The Hatchimals analysis was published on Sept. 17, 2019, and the Bubbu analysis on Oct. 14, 2019, both well after Google Play made the changes described above.

⁴² Swerve, About the Company, <https://www.swrve.com/company>.

⁴³ *See* 16 C.F.R. § 312.3.

after IDAC brought these apps to Google’s attention.⁴⁴ Several other apps by the same publishers remain on the Play Store.⁴⁵ This suggests that Google is not checking to make sure that apps participating in the Designed for Families program comply with its policies.⁴⁶

B. Some app developers and SDKs agreed to change their practices to settle multiple class actions lawsuits

Additional evidence of widespread non-compliance with COPPA by children’s apps comes from three related class actions brought by parents over gaming apps for kids. *McDonald v. Killoo* concerned the popular “Subway Surfers” app.⁴⁷ *Rushing v. The Walt Disney Company* involved “Princess Palace Pets” and four versions of “Where’s My Water?”⁴⁸ *Rushing v. Viacom Inc.* concerned “Llama Spit Spit.”⁴⁹ All three cases alleged that the apps tracked online behavior on a device and user-specific level and that Defendants exploited the data, without disclosure or consent, for profit. They asserted that this conduct violated COPPA and sought to enjoin these practices under state laws.

The Defendants in these cases fell into two different groups -- the “developer Defendants,” such as Disney and Viacom, and the “SDK Defendants.” The SDK Defendants were mobile advertising and app monetization companies that provide “software development kits” containing code to collect user data. Many of the SDKs named in these cases were also identified as likely violating the COPPA Rule in the 2018 Request.⁵⁰

⁴⁴ Ingrid Lunden, *Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations*, TechCrunch (Oct. 23, 2020), <https://techcrunch.com/2020/10/23/google-removes-3-android-apps-for-children-with-20m-downloads-between-them-over-data-collection-violations/>. The three apps -- Princess Salon, Number Coloring and Cats & Cosplay -- had more than 20 million downloads between them. *Id.*

⁴⁵ *Id.*

⁴⁶ According to the Android Developers Blog, Google uses machine learning to analyze apps before they are published in Google Play to protect users from harmful apps. Sai Deep Tetali, *Keeping 2 billion Android devices safe with machine learning* (May 24, 2018), <https://android-developers.googleblog.com/2018/05/keeping-2-billion-android-devices-safe.html>. However, it does not appear to be using this capability to identify and remove apps that do not comply with its Designed for Families criteria.

⁴⁷ *McDonald v. Killoo*, N.D. Cal. No. 3:17-cv-04344-JD.

⁴⁸ *Rushing v. Walt Disney Co.*, N.D. Cal. No. 3:17-cv-04419-JD.

⁴⁹ *Rushing v. ViacomCBS Inc.*, N.D. Cal. No. 3:17-cv-04492-JD.

⁵⁰ The SDKs named in the class action law suits were AdColony, Chartboost, Flurry, InMobi, ironSource, Tapjoy, Twitter, Vungle, Unity Ads, and Upsight. Plaintiffs’ Motion for Preliminary Approval of Class Action Settlements, N.D. Cal. No. 17-cv-04344-JD (filed Aug. 5, 2020) at 6 (“Motion for Approval”). CCFC/CDD’s FTC filing identified Ad Colony, ChartBoost, InMobi, Vungle and Unity Ads, as well as several others. 2018 Request at 14-15, n. 47, and Exhibits 2, 8, 9 & 10. The *IDAC Study* also identified several of the same SDKs as problematic. *IDAC Study* at 11.

Plaintiffs alleged that the SDK Defendants embedded code into the games to gather and transmit “persistent identifiers” and personal data for tracking, profiling and ad targeting.⁵¹ After the court denied Defendants’ motions to dismiss, the parties reached proposed settlements with all 16 Defendants.⁵² The Court approved the settlements in December 2020.⁵³

While the Defendants made no admissions of liability, the evidence presented, along with the extensive injunctive relief obtained for class members, suggests that the violations were widespread. For example, Class Counsel used forensic analysis to identify “tens of thousands of apps that (i) are featured in Google’s Designed for Families program, the Family section of Google Play, and the Kids Category of the Apple App Store; and (ii) contain these Defendants’ SDKs. Altogether, they identified 16,093 unique apps (with approximately 63,388 versions) across relevant SDK Defendants.”⁵⁴

The settlement will require the SDK Defendants, which “comprise a substantial share of the online ad network marketplace,”⁵⁵ to change their practices with regard to children’s apps. The SDK Defendants agreed to either stop advertising or limit their services to contextual advertising where a user is identified as under age 13.⁵⁶ Each SDK Defendant also agreed to either delete or refrain from disclosing, using, or benefiting from any personal data previously collected from child users in any apps identified above, with certain exceptions (*e.g.*, to comply with a Court order).⁵⁷ The agreements further require the SDKs to establish an enrollment process for developers and to screen for apps directed to children.⁵⁸

As discussed above, Google requires apps in the Designed for Families program to use certain SDKs. The approved SDKs include some of the Defendants in the class action cases, *i.e.*, AdColony, ChartBoost, inMobi, ironSource, Unity Ads, and Vungle.⁵⁹ While perhaps these SDKs have since come into compliance with COPPA, the agreement gives them 120 to 180 days after the settlement becomes final to comply. In any event, Google permits developers to use other SDKs that are not subject to settlement agreements.

In sum, facts uncovered in three class action cases, along with three recent studies, strongly suggest that many children’s apps on Google Play are not complying with the COPPA Rule. Thus, it is important that the FTC conduct its own investigation as to the truthfulness of Google Play’s representations regarding the Teacher approved and Designed for Families apps.

⁵¹ *McDonald v. Killoo*, 385 F.Supp.3d 1022, 1028 (N.D. Ca. 2019).

⁵² Plaintiffs’ Motion for Preliminary Approval of Class Action Settlements, N.D. Cal. No. 17-cv-04344-JD (filed Aug. 5, 2020) (“Motion for Approval”).

⁵³ The court granted preliminary approval in September 2020. *McDonald v. Killoo*, N.D. Cal. No. 17-cv-04344-JD, 2020 WL 5702113 (Sept. 24, 2020). Final approval was granted at a hearing held on December 17, 2020.

⁵⁴ Motion for Approval at 5.

⁵⁵ *Id.* at 7.

⁵⁶ *Id.*

⁵⁷ *Id.* at 6.

⁵⁸ *Id.* at 7.

⁵⁹ Participate in the Families Ads Program, <https://support.google.com/googleplay/android-developer/answer/9283445?hl=en>.

III. The need to investigate Google Play is even greater now because of the pandemic

As the FTC knows, children have substantially increased their use of and dependence on online media, including apps, as a result of the pandemic. A study by SuperAwesome found that the majority of US kids ages 6-12 “say they use screen devices either a lot more (at least 50% more), twice as much, or for what feels like ‘most of the day’ during the coronavirus pandemic.”⁶⁰ As Kidscreen explains, “games are increasingly becoming places where kids can meet and be social, doubling as networks over which they can connect with their friends at a distance. One in five US kids are using the in-game chat function while they play.”⁶¹

Another study, the 2021 Childwise Monitor Report, likewise found that kids are spending even more time online than last year. It found the biggest increase was among 11-to 12-year olds, who are now spending 4.2 hours a day online (compared to 3.3 hours previously). It also found the percentage of kids with internet access in their bedrooms increased from 80% to 83%, and “a whopping 73% of kids—and half of all five- to 10-year-olds—now own a mobile phone.”⁶² According to App Annie, educational apps have seen “phenomenal growth” since April 2020.⁶³ Google Play, in fact, introduced “Teacher approved” apps in response to this increased demand for child-appropriate apps.

Children’s increasing use of apps and other digital media has raised widespread concern about harms to children and families. For example, Dr. Dimitri Christakis, director of the Center for Child Health, Behavior and Development, notes that increased online use is associated with

⁶⁰ Sara Fischer, *Kids’ daily screen time surges during coronavirus*, Axios, Mar. 31, 2020, <https://www.axios.com/kids-screen-time-coronavirus-562073f6-0638-47f2-8ea3-4f8781d6b31b.html>.

⁶¹ Ryan Tuchow, *How gaming, interaction & influencers are merging*, Kidscreen, Nov. 25, 2020.

⁶² Elizabeth Foster, *Pandemic stress causes jump in screen time*, Kidscreen, Jan. 28, 2021, <https://kidscreen.com/2021/01/28/pandemic-stress-causes-jump-in-screen-time/>.

⁶³ In the US, “time spent in Education apps on Android phones grew 30% year over year during the week commencing Sept 6, 2020 compared to one year earlier.” Lexi Sydow, *Mobile Minute: Remote Return to School Sees 90% Boost Across Top Education Apps*, <https://www.appannie.com/en/insights/mobile-minute/top-education-apps-growth-2020/>. Another study by The NPD Group found that the number of US children ages 2 to 12 playing games on their phones climbed 9% from 2019 to 2020 and that COVID-19 was the main driver behind this growth. Ryan Tuchow, *Mobile gaming up 9% among kids*, Kidscreen, Jan. 19, 2021.

anxiety, depression, obesity, and aggression.⁶⁴ Another concern is the cost of in-app purchases.⁶⁵ According to the Kids' Allowance Report, "children's spending habits have changed significantly since lockdown was implemented earlier this year. Old favorites like candy and books/magazines are no longer priorities, with many kids shifting their dollars to online games like *Roblox* and *Fortnite*."⁶⁶

While the FTC has brought a few enforcement actions against developers of children's apps,⁶⁷ its whack-a-mole approach cannot fix the systemic problem that Google Play, the largest source of apps for children, misrepresents children's apps as complying with COPPA when they do not. Thus, it is important that the FTC conduct a thorough review of Google Play's practices regarding children's apps.

IV. Section 230 does not prevent the FTC from finding that Google Play violated Section 5

Should the FTC's investigation confirm that Google's representations that child-directed apps on the Play Store are appropriate for children and comply with COPPA are false or

⁶⁴ Matt Richtel, *Children's Screen Time Has Soared in the Pandemic, Alarming Parents and Researchers*, NY Times (Jan. 16, 2021), <https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.html?searchResultPosition=2>. Keith Humphreys, a professor of psychology at Stanford University and an expert on addiction, predicts that "[t]here will be a period of epic withdrawal" when young people will need to "sustain attention in normal interactions without getting a reward hit every few seconds." *Id.*

⁶⁵ E.g., Emily Flake, *My Kid Sold Her Soul to Roblox*, NY Times, Sept. 23, 2020, <https://www.nytimes.com/2020/09/23/parenting/roblox-screentime.html> (describing a friend who forbade his son from using Roblox after he made \$700 worth of in-app purchases).

⁶⁶ Elizabeth Foster, *Kids spending shifts to online games*, Kidscreen, Sept. 16, 2020. The Roblox app, which is "particularly popular among children ages 9 to 12 in the United States, averaged 31.1 million users a day during the first nine months of 2020, an increase of 82 percent over the year before." Richtel, *supra* note 3.

⁶⁷ *United States v. HyperBeard, Inc.*, No. 3:20-cv-3683 (N.D. Ca. June 30, 2020)(defendants offered mobile apps directed to children on Google Play that collected children's personal information without notice and verifiable parental consent); *Miniclip. S.A.*, No. C-4722 (FTC June 29, 2020)(distributor of child-directed apps on Google Play violated §5 for falsely representing that it was a participant in the CARU COPPA safe harbor program); *U.S. v. InMobi Pte Ltd.*, No 3:16-cv-3473 (N.D. Ca. June 22, 2016) (mobile advertising network providing SDKs to app developers knowingly tracked geolocation and served behavioral ads to children without providing direct notice to parents or obtaining verifiable consent from parents); *US v. LAI Systems, LLC*, No. 2:15-cv-9691 (C.D. Ca. Dec. 17, 2015)(seller of children's mobile apps violated COPPA by failing to give parental notice and obtain parental consent); *US v. Retro Dreamer*, No. 5:15-cv-2569 (C.D. Ca. Dec, 17, 2015)(defendant offered apps directed to children on Google Play that allowed third party ad networks to collect personal information without notice or parental consent); *United States v. TinyCo*, No. 3:14-cv-04164, (N.D. Ca. Sept 16, 2014) (company offering mobile apps for kids on Google Play collected email addresses from children without providing notice and obtaining verifiable consent from parents).

misleading, Section 230 of the Communications Act would not prevent the FTC from taking appropriate action against Google Play.

Section 230(c)(1), known as the liability shield, states that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”⁶⁸ When determining the applicability of Section 230, courts apply a three-part test which evaluates:

- whether the party asserting Section 230 is a person or entity covered by the provision (i.e., an interactive computer service or a user of an interactive computer service);
- whether the content at issue was developed by another information content provider; and
- whether the claims asserted seek to hold the party liable as though they were the speaker or publisher of the content at issue.⁶⁹

Section 230 provides a shield only if all three prongs are met. Assuming Google Play is an interactive computer service and would meet the first prong, the other parts of the test would not be satisfied. The second prong, that the content was developed by another information content provider, is not satisfied because the information content at issue consists of statements made by Google Play on its platform, in its Parent’s Guide, and in its blog.

Nor would the third prong be met because the FTC would not be treating Google Play as a publisher of the content of another. It is Google’s own representations about Teacher approved and Designed for Families apps in the Play Store that are deceptive. An action against Google Play for unfair or deceptive practices would seek to hold Google Play liable for its own speech, not the speech of third parties. This result is consistent with the only two court cases where defendants tried to claim §230 immunity to the FTC’s allegations of unfair or deceptive practices. In each case, the court rejected immunity on the ground that the defendant was liable for its own deceptive acts or practices rather than for publishing content created by another.⁷⁰

Nor would Google be able to take advantage of Section 230(c)(2), known as the Good Samaritan provision, that states that “No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.”⁷¹ Here, no one is claiming that Google Play is restricting access to

⁶⁸ 47 U.S.C. §230(c)(2).

⁶⁹ E.g., *Jane Doe No. 1 v. Backpage.com*, 817 F.3d 12, 19 (1st Cir. 2016); see also Kathleen Ann Ruane, *How Broad a Shield? A Brief Overview of Section 230 of the Communications Decency Act*, Cong. Res. Serv., Feb. 21, 2018, at 1-2.

⁷⁰ *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173-77 (2d Cir. 2016); *FTC v. AccuSearch, Inc.*, 570 F.3d 1187, 1199-1201 (10th Cir. 2009).

⁷¹ 47 U.S.C. §230(c)(2).

apps, much less on its belief that they are “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” Rather, the claim is that Google represents certain apps are appropriate for children under 13 when they are not because they do not comply with the requirements of COPPA.

Conclusion

Because of the pandemic, children are using more mobile apps and for longer periods of time. Google Play touts its Teacher approved apps as helping parents find “the good stuff” for their kids during the pandemic. Its policies also require that apps that target children, even as only part of their audience, must be appropriate for children and comply with COPPA. Yet, three recent studies, as well as facts uncovered in three class action lawsuits, strongly suggest that some of these apps do not comply with the COPPA Rule. Thus, we urge the FTC to investigate Google’s practices and the truthfulness of its representations and act to protect parents from being misled and children from playing apps that are not appropriate and violate their privacy.

Respectfully submitted,

Campaign for a Commercial-Free Childhood
Center for Digital Democracy

cc: Daniel Kaufman, Acting Director of the Bureau of Consumer Protection
Maneesha Mithal, Associate Director, Division of Privacy & Identity Protection

Find high-quality apps for kids on Google Play

 blog.google/products/google-play/teacher-approved-apps

April 15, 2020

Families



Mindy Brooks

Product and UX Director, Kids and Families

Published Apr 15, 2020

We've heard from parents that it's difficult to dig through all the content that's out there for kids. Today, we're making it easier for parents to find the good stuff, with a new Kids tab on Google Play filled with "Teacher approved" apps that are both enriching and entertaining. We decided to launch the Kids tab a bit earlier than planned because parents who have tried it out told us that it's been helpful, especially now with their kids home from school and spending more time with screens. Because it's early, you may not see some of your favorite apps in there just yet, but we're adding new content as quickly as possible.

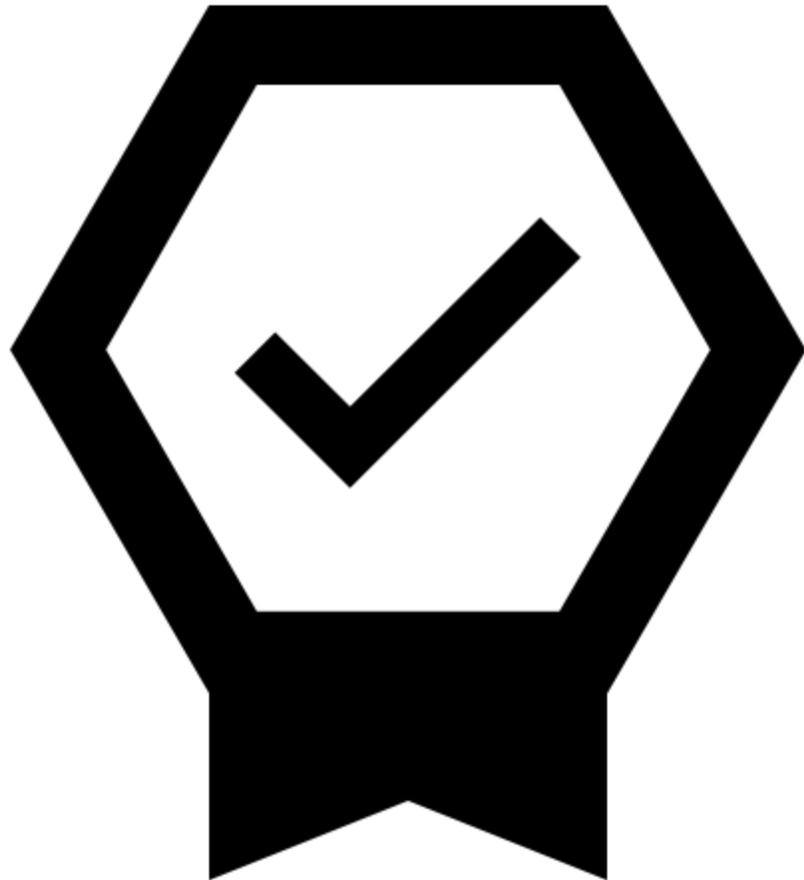


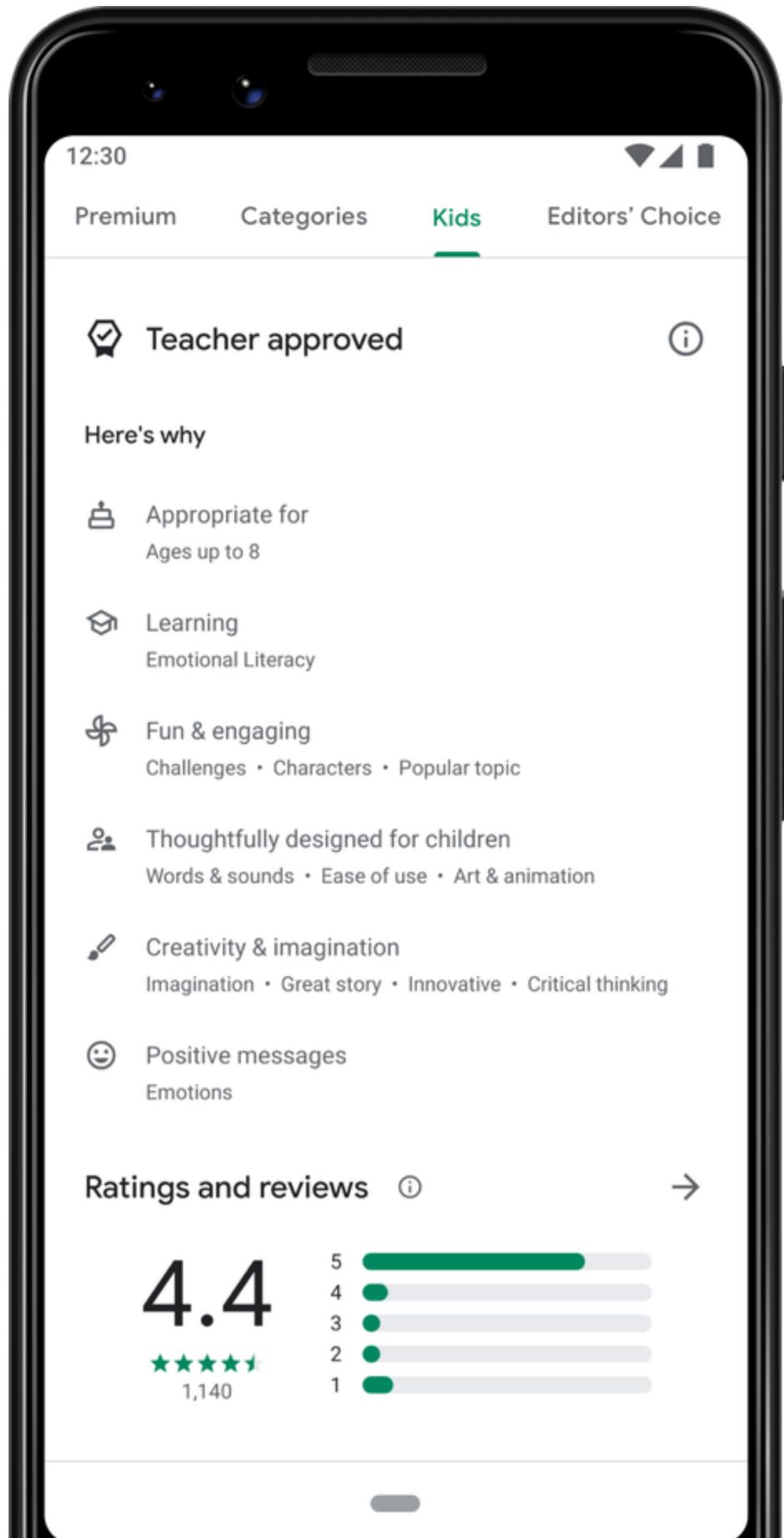
"Teacher approved" kid-friendly app content

Exhibit A

Great content for kids can take many forms: Does it spark curiosity? Does it help your child learn? Is it just plain fun? To share the best apps for kids on the Play Store, we've teamed up with academic experts and teachers across the country, including our lead advisors, Joe Blatt (Harvard Graduate School of Education) and Dr. Sandra Calvert (Georgetown University). Apps that have been rated by teachers and meet our quality standards receive a "Teacher approved" badge.

Apps are rated on factors like age-appropriateness, quality of experience, enrichment, and delight. We include information in the app listing about why the app was rated highly to help parents determine if the app is right for their child.







How to find “Teacher approved” apps in Google Play

Whenever parents search the Play Store, they can look for the “Teacher approved” badge to quickly see which apps have been reviewed and rated highly by teachers. If you want to browse content that's been “Teacher approved”, simply go to the ["Kids" tab](#). And, if you're a [Google Play Pass](#) subscriber, a great selection of “Teacher approved” content is available within “Apps and games for kids.”

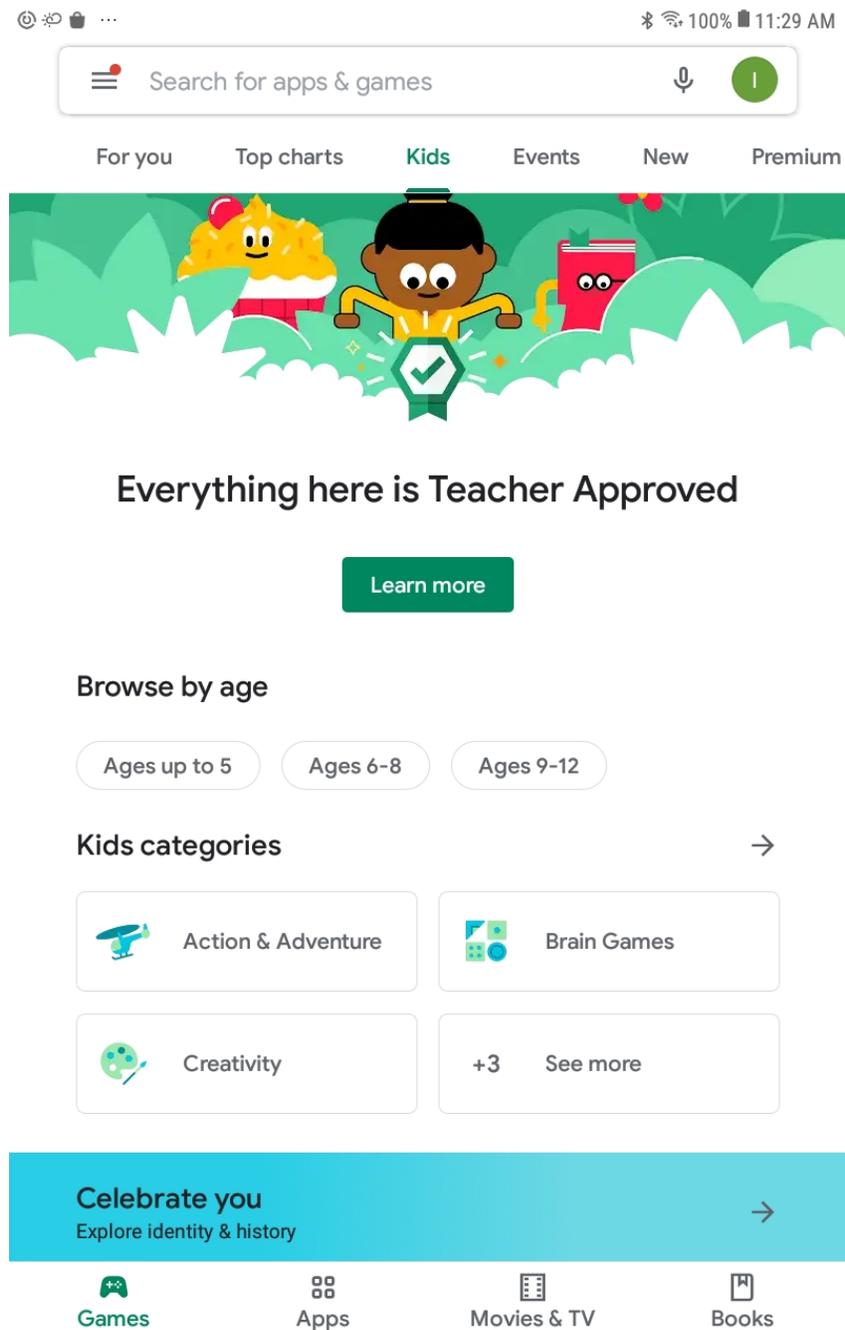
Today's announcement wouldn't be possible without [teachers who've been working closely with us](#) for the last few years to curate apps that can help kids develop, grow and have fun. We trust teachers to enrich our kids while they're in school, and we're grateful they've shared their expertise to rate the apps kids use when they're not in school as well.

The new Kids tab with “Teacher approved” apps will roll out in the U.S. on Google Play over the next few days, and we'll be expanding internationally in the coming months. We'd love to hear what you think as we continue to make the Play Store more helpful for parents. You can share your thoughts by opening the menu in the Play Store and tapping “Help and feedback.” And don't forget—for parents who want to set digital ground rules for their kids, like setting time limits on the apps your child has on their device, check out our [Family Link](#) app.

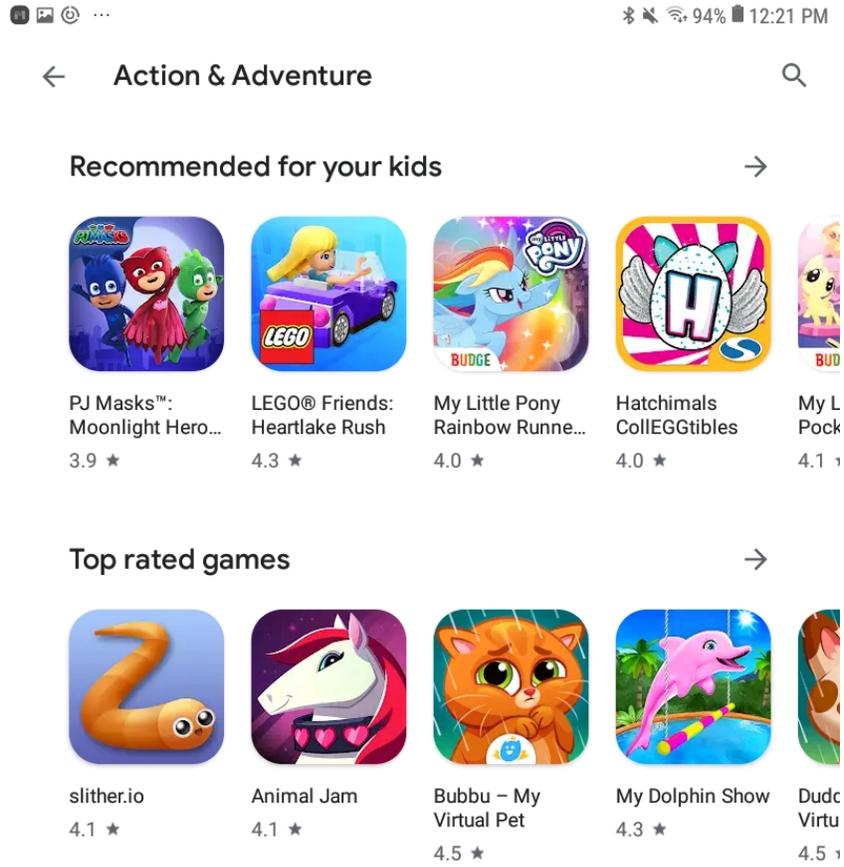
Exhibit B

Examples of a Teacher approved app and a child-directed (but not Teacher approved app)
Screen shots taken March 1, 2021 on a Galaxy Samsung Tablet.

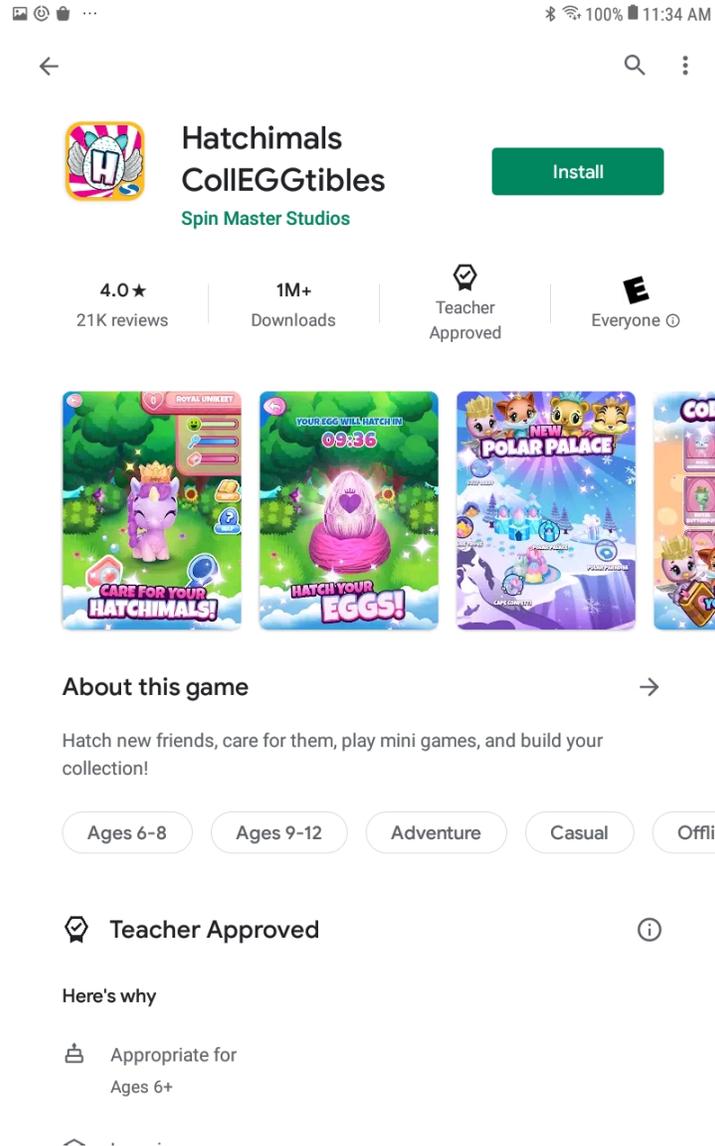
Let's say a parent is looking for virtual pet for their child. They go to Google Play and click on the kids tab.



The parent selects Action & Adventure, and receives the following recommendations, which include two virtual pet games -- Hatchimals CollEGgtibles and Bubbu - My Virtual Pet.



Wanting to know more, the parent clicks on each icon. This is what the parent sees after clicking on Hatchimals COLLEGGtibles. Note that it displays the Teacher approved badge and is rated E for everyone.



This is what the parent sees when clicking on Bubbu - My Virtual Pet. It too is rated E for everyone, and appears to child-directed, but it does not have the Teacher-approved badge.

The screenshot shows the Google Play Store interface for the app 'Bubbu - My Virtual Pet'. At the top, there are navigation icons (back, search, menu) and system status icons (signal, Wi-Fi, 100% battery, 11:34 AM). The app's icon, a cute orange cat, is on the left. To its right is the title 'Bubbu - My Virtual Pet' and a green 'Install' button. Below the title is the developer name 'Bubadu' and the text 'Contains ads • In-app purchases'. The app has a 4.5 star rating from 800K reviews, over 50M downloads, and an 'E' rating for 'Everyone'. Two preview images are shown: one of the cat in the rain and another of the cat in a bathroom. Below the images is the 'About this game' section, which includes the description 'Adopt a new cat, Bubbu, and become his best friend.' and genre tags: 'Casual', 'Simulation', 'Care', 'Casual', and 'Offline'. The 'Ratings and reviews' section shows a 4.5 star average with a bar chart indicating the distribution of ratings from 1 to 5 stars, based on 800,551 reviews.

4.5 ★
800K reviews

50M+
Downloads

E
Everyone

BUBBU
my virtual pet

About this game

Adopt a new cat, Bubbu, and become his best friend.

Casual Simulation Care Casual Offline

Ratings and reviews

4.5
★★★★★
800,551

Rating	Count
5	~65%
4	~25%
3	~5%
2	~2%
1	~3%

Parent Guide to Google Play

 support.google.com/googleplay/answer/6209547

Explore the topics below to learn about features for parents in Google Play.

Find content for kids

1. On your Android phone or tablet, open the Google Play Store .
2. Tap **Games**, or **Apps**.
At the top, tap **Kids**.
All apps in this section are Teacher Approved. [Learn more about the Teacher Approved badge](#).
3. For Movies & TV, tap **Family**.
4. For Books, tap **Children's Books**.

[Learn more about finding family-friendly content](#).

Ads in Kids apps

Ads are expected to be consistent with the maturity rating of the app or game. Ad serving can change over time so you should check what types of ads are being shown from time to time.

If you see ads that aren't appropriate for the age group the app was designed for, [report the ad to Google](#).

Use parental controls to restrict mature content

If you share your Android phone or tablet with others, including kids, you can turn on parental controls to block downloads or purchases of content based on the content maturity level. You can choose different parental control settings for each type of content, and for each device.

[Learn more about setting up parental controls](#).

Prevent accidental purchases with password protection

To help prevent accidental or unwanted purchases on your device, authentication is required before any purchases, including in-app purchases, are made from any apps available in the Kids section, even if you don't usually require one.

Exhibit C

[Learn more about passwords and authentication.](#)

Use Google Play Family Library

You can share purchased apps, games, movies, TV shows, and books from Google Play with up to 5 other family members once you set-up Google Play Family Library.

[Learn more about family library.](#)

Was this helpful?

Find family-friendly content in Google Play

 support.google.com/googleplay/answer/6209531

Google Play reviews apps for certain [policy requirements](#), but developers can make changes to their apps anytime. It is important that parents review all information about an app before downloading to make sure that the app is appropriate for their child.

Find games or apps for kids

1. On your Android phone or tablet, open the Google Play Store .
2. Tap **Games**, or **Apps**.
At the top, tap **Kids**.
All apps in this section are Teacher Approved. [Learn more about the Teacher Approved badge](#).
3. For Movies & TV, tap **Family**.
4. For Books, tap **Children's Books**.

Tip: To prevent anyone who uses your device from downloading or purchasing mature content, [set up parental controls](#).

What the “Teacher Approved” badge means

Google consulted with academic experts to develop a framework for rating apps, and then worked with teachers and specialists across the US to rate them based on our framework.

Teacher Approved apps are:

- Age appropriate
- Thoughtfully designed
- Fun or inspiring

Teachers and specialists only rate apps for the age groups that they teach and they have all been vetted, trained, and evaluated before they become part of the program. Currently, the team is not hiring teachers or specialists outside of the program.

Tip: Apps are updated regularly and teachers and specialists review apps on an ongoing basis. This means that apps that are Teacher Approved will change over time.

Age ranges for Movies & TV and Books

Check an app's privacy policy

Exhibit C

All apps and games in the Kids section have to include a link to their privacy policy at the bottom of the app details page.

We recommend that you review the privacy policy before downloading the app to learn how the app collects and uses personal information.

Report inappropriate content

We do our best to make sure family-friendly content meets Google Play's heightened policy requirements.

If you find content that may be inappropriate for kids and families, [let us know](#).

Related articles:

Was this helpful?

Exhibit D

App Census analysis of Hatchimals

AppSearch Search for Android apps in our analysis database

Hatchimals COLLEGGtibles
 Developers: Spin Master Studios
 Privacy Policy
 Version 1.9.6
 Published on 09/17/2019
 Action & Adventure • Adventure

Transmits Sensitive Data

Permission-Protected Resources

In order for an app to access sensitive resources in Android (e.g., personally identifiable information, camera and microphone, etc.), it must first request permission. The tables below list the permission-protected sensitive resources that this app had permission to access and whether we observed it actually accessing them. In some cases, this might be due to the app requesting access to more data than it actually needs to function, though in other cases it may be due to our testing mechanisms not triggering the relevant app functionality (which may be triggered with additional testing).

Resources Accessed lists the data types that we observed the app accessing during our testing.

Resources Requested lists the data types that the app could have accessed, but never actually accessed during the testing period.

Warning: just because we did not observe a particular permission-protected data type being accessed during our limited testing period does not mean that the app definitively will not access it when tested under different conditions.

Resources Accessed	Resources Requested
No permission-protected resources accessed during our testing.	No unused permission-protected resources requested by this app.

Detected Data Flows

During our testing, we examined whether this app transmitted any personal information (e.g., your name, location, or contact information) or device identifiers. Device identifiers are pieces of information unique to you (e.g., an account number) or your smartphone (e.g., a serial number) that can be used to track your behaviors over time. Various advertisers and analytics services may do this to profile you based on your usage habits, such as what apps you use. The use of device identifiers is very similar to how websites use cookies. Information types that we did not observe being transmitted during our testing are shown greyed out below.

Warning: just because we did not observe a particular data type being transmitted during our limited testing period does not mean that the app definitively will not transmit it when tested under different conditions.

Personal Information

AppSearch Search for Android apps in our analysis database

Device Identifiers

IMEI, Android ID, GSF ID, SERIAL #

Data Recipients

When this app transmits sensitive information, it is received by the parties listed in the table below. The second column indicates the data type each party receives, and the third column indicates whether or not the data was encrypted while in transit using TLS.

Warning: just because we did not observe a particular data type being transmitted during our limited testing period does not mean that the app definitively will not transmit it when tested under different conditions.

Domain	Info Shared	Encrypted?
4574.content.surve.com	Device Description	Yes
ctp.cloud.unity3d.com	Advertising ID	Yes
ctp.cloud.unity3d.com	Android ID	Yes
ctp.cloud.unity3d.com	Device Description	Yes
config.usa.cloud.unity3d.com	Android ID	Yes

AppCensus Analysis of Bubba

AppSearch Search for Android apps in our analysis database



Bubba - My Virtual Pet

Developer: Bubadu
[Privacy Policy](#)

Version 1.68
 Published on 10/14/2019
 • Casual •



Transmits Sensitive Data

Permission-Protected Resources

In order for an app to access sensitive resources in Android (e.g., personally identifiable information, camera and microphone, etc.), it must first request *permission*. The tables below list the permission-protected sensitive resources that this app had permission to access and whether we observed it actually accessing them. In some cases, this might be due to the app requesting access to more data than it actually needs to function, though in other cases it may be due to our testing mechanisms not triggering the relevant app functionality (which may be triggered with additional testing).

Resources Accessed lists the data types that we observed the app accessing during our testing.

Resources Requested lists the data types that the app *could* have accessed, but never actually accessed during the testing period.

AppSearch Search for Android apps in our analysis database






Device Identifiers










Data Recipients

When this app transmits sensitive information, it is received by the parties listed in the table below. The second column indicates the data type each party receives, and the third column indicates whether or not the data was encrypted while in transit using TLS.

Warning: just because we did not observe a particular data type being transmitted during our limited testing period does not mean that the app *definitely* will not transmit it when tested under *different* conditions.

Domain	Info Shared	Encrypted?
auction.unityads.unity3d.com	Advertising ID	Yes
publisher-config.unityads.unity3d.com	Advertising ID	Yes
settings.crashlytics.com	Device Description	Yes
vast.kidoz.net	Advertising ID	Yes