MOBILE APPS: GOOGLE VS. APPLE COPPA SCORECARD (CHILDREN’S PRIVACY)

Q1.2022

An analysis of child-directed* mobile apps across the Google and Apple app stores

* Based on Pixalate’s methodology
A NOTE ABOUT COPPA

The Children's Online Privacy Protection Act ("COPPA") is a United States federal law passed by Congress in 1998 to protect children's online privacy. COPPA required the Federal Trade Commission ("FTC") to issue and enforce a rule implementing the law. The FTC's COPPA Rule (the "Rule") became effective in 2000, and it was amended in 2013. The FTC is presently in the process of reviewing the Rule again. COPPA is enforced by the FTC and by state Attorneys General, who have the authority to seek civil penalties from companies that violate the Rule.
**KEY STATS: THE STATE OF CHILD-DIRECTED MOBILE APPS IN Q1 2022**

AS MEASURED BY PIXALATE

- There are **>391k child-directed** mobile apps across Google and Apple stores
- **8%** of Apple App Store apps and **7%** of Google Play Store apps are child-directed*
- **~40%** of child-directed* mobile apps have potential access to personal info***
- Programmatic advertisers spent **3.1x more** per app on child-directed* apps than on general audience apps**
- **12k** child-directed apps have potential access to personal info*** but have no detected privacy policy
- Personal info*** is **42% more likely** to be shared w/ advertisers on child-directed apps

---

* Based on Pixalate’s [methodology](#).

** General audience is the term used by the FTC to describe sites and services that do not target children under 13 as a portion of the audience. See the FTC’s 1999 [Statement of Basis and Purpose](#).

*** Geolocation info, persistent identifiers such as IP address or unique device identifier, and photo, video or audio files containing a child’s image or voice are all considered personal info under COPPA. See the [COPPA Rule](#) at 16 C.F.R. § 312.2 for more.
# Google vs. Apple: Scorecard for Children’s Privacy (Q1 2022)

As of the end of Q1 2022; as scored by Pixalate

<table>
<thead>
<tr>
<th>Child-Directed Apps With...</th>
<th>Google</th>
<th></th>
<th>Apple</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>226,483</td>
<td>7% of all apps</td>
<td>165,172</td>
<td>8% of all apps</td>
</tr>
<tr>
<td>Undetected Privacy Policy</td>
<td>24,974</td>
<td>11% of child-directed</td>
<td>34,824</td>
<td>21% of child-directed</td>
</tr>
<tr>
<td>Potential Personal Info Access</td>
<td>98,948</td>
<td>44% of child-directed apps</td>
<td>64,780</td>
<td>39% of child-directed apps</td>
</tr>
<tr>
<td>GPS Transmitted to the Ad Industry</td>
<td>11,628</td>
<td>5% of child-directed</td>
<td>6,907</td>
<td>4% of child-directed</td>
</tr>
<tr>
<td>Residential IP Transmitted to the Ad Industry</td>
<td>11,067</td>
<td>5% of child-directed</td>
<td>6,289</td>
<td>4% of child-directed</td>
</tr>
<tr>
<td>Request Camera Access</td>
<td>62,641</td>
<td>28% of child-directed</td>
<td>44,476</td>
<td>27% of child-directed</td>
</tr>
<tr>
<td>Undetected Privacy Policy &amp; Camera Access</td>
<td>19</td>
<td>0.01% of child-directed</td>
<td>4,460</td>
<td>2.7% of child-directed</td>
</tr>
<tr>
<td>Undetected Privacy Policy &amp; Potential Personal Info Access</td>
<td>2,178</td>
<td>1% of child-directed</td>
<td>9,819</td>
<td>5.9% of child-directed</td>
</tr>
<tr>
<td>Undetected Privacy Policy &amp; GPS Transmitted</td>
<td>517</td>
<td>0.2% of child-directed</td>
<td>517</td>
<td>(0.4% of child-directed)</td>
</tr>
<tr>
<td>Undetected Privacy Policy &amp; Res. IP Transmitted</td>
<td>635</td>
<td>0.3% of child-directed</td>
<td>1,180</td>
<td>(0.7% of child-directed)</td>
</tr>
<tr>
<td>Undetected Privacy Policy &amp; Potential Personal Info Access &amp; GPS &amp; Res. IP Transmitted</td>
<td>34</td>
<td>(0.02% of child-directed)</td>
<td>132</td>
<td>(0.1% of child-directed)</td>
</tr>
</tbody>
</table>

Chart shows # of child-directed apps and overall % of child-directed apps in parenthesis.
CHILD-DIRECTED APPS ON THE GOOGLE & APPLE APP STORES

The scale of child-directed apps and how often personal data is shared on those apps
~8% of all apps (7.2% on Google Play Store and 8.3% on Apple App Store) are child-directed as of Q1 2022, according to Pixalate’s data.

Want to see all the apps? Schedule a demo: pixal.at/demo
Of the top 1k most popular apps in the Google Play Store transmitted location and personal IP addresses in the ad bid stream during Q1 2022, according to Pixalate’s data.

Want to see all the apps? Schedule a demo: pixal.at/demo
3.1x more ad spend per app on child-directed apps (compared to general audience apps) in Q1 2022, according to Pixalate’s estimates.

Want to see all the apps? Schedule a demo: pixal.at/demo
Child-directed apps are more likely to share sensitive user data with advertisers among apps with programmatic ads in Q1 2022; as measured by Pixalate.

Child-directed apps are 42% more likely to share both GPS and IP address with third-party digital advertisers than non-child-directed apps.
>248K CHILD-DIRECTED APPS FROM UNKNOWN COUNTRIES
AS OF THE END OF Q1 2022; AS MEASURED BY PIXALATE

+4%

~4% increase in the # of child-directed apps across Google/Apple app stores with either no country of registration or a country of registration that was not identifiable by Pixalate

Want to see all the apps? Schedule a demo: pixal.at/demo
THE DATA ‘DARK ZONE’ ON CHILD-DIRECTED APPS

Apps with no detected privacy policy but access to and/or transmission of personal information
>40% OF CHILD-DIRECTED APPS HAVE POTENTIAL ACCESS TO PERSONAL INFO VIA DEVICE PERMISSIONS

AS OF THE END OF Q1 2022: AS MEASURED BY PIXALATE

* Geolocation information, persistent identifiers such as IP address or unique device identifier, and photo, video or audio files containing a child’s image or voice are all considered personal information under COPPA. See COPPA Rule at 16 C.F.R. § 312.2 for more.

~40% of child-directed apps across Google/Apple have potential access to personal information through the device permissions they request

Want to see all the apps? Schedule a demo: pixal.at/demo
~12K Child-Directed Apps Have Potential Access to Personal Info But No Detected Privacy Policy
As of the end of Q1 2022: As Measured by Pixalate

Child-directed apps across Google/Apple have potential access to personal information but no detected privacy policy as of Q122 (a slight improvement from 12.7k such apps in Q421)

Want to see all the apps? Schedule a demo: pixal.at/demo
METHODOLOGY & DISCLAIMER
General
Pixalate’s data science and analyst team analyzed apps available for download via the Apple App Store and Google Play Store as of the last date of Q1 2022 (March 31); data derived from crawls of the respective app stores performed by Pixalate or one of Pixalate’s third party licensors.

Country of Registration
The country of registration for a given app is determined only if a) the app has a physical address published in its app store page, or otherwise b) from the registrant physical address of the publisher domain listed in the app store page excluding privately registered ones. If none of them is available, the physical address associated with an app cannot be determined. Sometimes, the same developer may list different countries of registration for different apps.

Child-Directed Apps
Pixalate uses automated processing derived from a combination of signals (which at times is coupled with human intervention) to determine if an app is likely to be child-directed, including the app’s category, sub-category, content rating, and contextual signals (specifically, child-related keywords in app’s title or the app’s description). See our full methodology for more.

General Audience Apps
General audience is the term used by the FTC to describe sites and services that do not target children under 13 as a portion of the audience. See the FTC’s 1999 Statement of Basis and Purpose.

Personal Data
Mobile apps request access to certain device permissions in order to operate, such as access to location services, access to the contact list, etc. In many cases, not all the permissions are used by the app that requests access to them, and very often, many permissions requested
Personal Data (continued)

might not even be needed for the normal operation of the app (e.g. GPS coordinates might be necessary for a weather app, but not for a drawing app). However, the fact that access to certain permissions has been requested creates additional risks since the permissions can be used at any time in the future. Pixalate has classified the most common mobile apps in terms of their COPPA risk, i.e. the risk to expose sensitive data. The COPPA sensitive permissions highlighted in this report include access to the device’s camera and access to the device’s location (including latitude and longitude coordinates). See the full list here.

Privacy Policy

An app is considered to have a detectable Privacy Policy if crawls of the Google or Apple app stores from Pixalate or one of Pixalate’s third party licensors found proof of a privacy policy. Otherwise, the app is considered to have either no or an undetected Privacy Policy.

Estimated Ad Spend

Pixalate calculates estimated programmatic ad spend through statistical models that incorporate programmatic monthly active users (MAU), the average session duration per user, the average CPM for the category of a given app, and ad density.
DISCLAIMER

The content of this report reflects Pixalate’s opinions with respect to the factors that Pixalate believes can be useful to the digital media industry. Any data shared is grounded in Pixalate’s proprietary technology and analytics, which Pixalate is continuously evaluating and updating. Pixalate’s opinions are just that, opinions, which means that they are neither facts nor guarantees.

It is important to note that the mere fact that an app appears to be directed to children (e.g., data subjects under 13 years of age, as defined by COPPA), does not mean that any such app, or its operator, is failing to comply with COPPA. Further, with respect to apps that appear to be directed to children and have characteristics that, in Pixalate’s opinion, may trigger related privacy obligations and/or risk, such assertions reflect Pixalate’s opinions (i.e., they are neither facts nor guarantees); and, although Pixalate’s methodologies used to render such opinions are derived from automated processing, which at times is coupled with human intervention, no assurances can be – or are – given by Pixalate with respect to the accuracy of any such opinions.

Pixalate is sharing this data not to impugn the standing or reputation of any entity, person or app, but, instead, to render opinions and report trends pertaining to apps available for download via the official Apple App Store and Google Play Store.

Apple and the Apple logo are trademarks of Apple Inc. Android and Google Play are trademarks of Google LLC. “Android robot” by Google LLC is licensed under CC BY 3.0.
ABOUT PIXALATE

Pixalate is the market-leading fraud protection, privacy, and compliance analytics platform for Connected TV (CTV) and Mobile Advertising. We work 24/7 to guard your reputation and grow your media value. Pixalate offers the only system of coordinated solutions across display, app, video, and OTT/CTV for better detection and elimination of ad fraud. Pixalate is an MRC-accredited service for the detection and filtration of sophisticated invalid traffic (SIVT) across desktop and mobile web, mobile in-app, and OTT/CTV advertising. www.pixalate.com

www.linkedin.com/company/pixalate/
https://www.facebook.com/pixalate
twitter.com/pixalateinc
THANK YOU!

info@pixalate.com
pixalate.com