BBB National Programs

Risky Business

The Current State of Teen Privacy in the Android App Marketplace

The data flows that power today's digital environment move across generations and cultures, devices and software, businesses and households. Many of the currents that feed into this environment are generated by the mobile app ecosystem, where users of all backgrounds engage with their favorite games, social media, tools, and entertainment sources.

Teenagers are major participants in this ecosystem. And like everyone else interacting with today's connected world, teenagers are faced with questions and tradeoffs when it comes to the use of mobile apps and privacy.

In policy discussions about privacy today, however, much of the dialogue focuses on the privacy rights of citizens generally—sometimes through the vehicle of general privacy regulation, and sometimes through protections for specific kinds of data, such as health data or location data. Also common are discussions about prioritizing the privacy interests of young children and whether existing legal frameworks, such as the Children's Online Privacy Protection Act[1] (COPPA), are adequate and sustainable in today's digital world.

Table of Contents

The Missing Link in Policy Discussions: Teens

The unique privacy interests of teenagers, a significant part of the U.S. population,[2] are rarely included in these privacy policy dialogues. This white paper aims to address this shortcoming.

83%
of U.S. mobile device owners aged 13 to 17 download an app at least once a month[3]

81%
of teens use social media with 70% saying they use it multiple times a day, up from 34% in 2012[4]

72%
of teens believe that tech companies manipulate users to spend more time on devices[5]

89%
of teens have their own smartphone, more than doubling since 2012[6]

To protect teen privacy interests, some lawmakers are proposing to raise the protected age range under COPPA to include teens[7] This year alone, we have seen the PROTECT Kids Act, the Kids PRIVACY Act, and the KIDS Act each applying certain concepts from COPPA to children under the ages of 16 or 17.

The ideas are worthy, but the specifics are lacking. The unique teen audience is strikingly different than COPPA's current targeted age range of under 13. Defining a website, app, or platform as a "teen space" is much more complex than identifying child-directed content. Teens occupy an intermediate space between childhood and adulthood, which demands a nuanced approach to setting new standards, not merely changing the age limit under COPPA.

Research shows that a teen's drive for greater engagement on digital media platforms exposes them to privacy risks.[8] There is a critical need to ensure that companies engaging teens in an online environment collect data in a responsible manner, understand the unique teen audience, and have the tools and support necessary to sustain responsible data collection in an evolving regulatory atmosphere.

Key Findings

To assess the multiple privacy dimensions of more than 53,000 apps available in the Google Play store, the apps were divided into two categories: apps directed to a general audience, and a subset of those that were directed to teens.

The data indicate that Android-based apps likely directed to teens differ substantively from general audience apps where information privacy is concerned.

Teen apps have a greater attack surface for privacy risks.

The teen dataset requested more permissions of its users and included more in-app purchase options than apps in the general dataset. And in 9% of apps in the teen dataset we were unable to identify a home country for the app publisher.

11	6	10
median permissions requested per app	median "dangerous" permissions requested per app	median trackers integrated into each app

Trackers observed most frequently appeared to be controlled by Facebook and Google.

The Android mobile app ecosystem is complex, populated by a variety of publishers that often rely on third-party software to monetize their apps through advertising or in-app purchases.

Apps function alongside powerful sensor, storage, and tracking technologies engineered into smartphones. Google, the owner of the Android platform and a powerful advertising network, and Facebook, known for its social media networks, dominate this market through myriad tracking and ad products. Such major players are woven together with innumerable advertising technology companies to create an interlocking mesh of data exchange that funds an enormous swath of internet services.

Many consumers, including teens, engage with their favorite apps every day unaware of the hidden ecosystem that drives them.

Teen users might be targeted based on their in-app purchase spending behavior.

The teen dataset included more ad-supported apps than the general dataset.

82%

of teen-directed apps

were supported by ads, compared to

51%

of general apps

Games for teens were more likely to have in-app purchases than game apps in the general dataset.

General Dataset

4:1 ratio of game apps with in-app purchases to those without

Teen Dataset, almost

13:1 ratio of game apps with in-app purchases to those without

Why it Matters

Apps targeted to teenage users are more likely to engage in ad serving, include more third-party trackers, ask for more permissions, and offer more in-app purchases.

App developers, advertisers, and third-party technology companies routinely focus more heavily on monetizing teenage users, through advertisements and in-app purchases, as compared to general audience users. In addition, the teen dataset included more third-party trackers and requested more permissions to data, including those defined as “dangerous” permissions. While many app developers appear to abide by the Google Play Developer policies about privacy, our study suggests there are important questions about whether they collect or authorize the collection of excessive amounts of data.

And because Google and Facebook own the majority of trackers in teen apps, this report demonstrates how platforms such as these can combine data, collected across a variety of apps, to create a full profile of single users – what they look like, what they sound like, where they go, who their friends and family are, where they work and live, their daily habits and interests, and even the contents of their phone.

In a world where teens are restricted from driving, voting, and making other decisions regarding their autonomy, why does the assumption exist that they can properly manage their own data privacy?

In today's landscape, should teens be required to understand and be mindful of the inherent tradeoffs that exist between the data collection and advertising practices in the mobile apps they use and their own personal privacy?

Although the proposed laws that expand the scope of COPPA to include some teenagers are well-intentioned, we should not treat teens the same way we treat children, nor should we treat them as fully developed adults.

Given our findings and the potential rigidity of future legislative solutions, it is incumbent on industry now to exercise responsibility and show accountability by developing appropriate standards that take into account teens' habits, preferences, and developmental state.

This study is brought to you by BBB National Programs' TeenAge Privacy Program (TAPP), a community of companies that understand the digital landscape and the complications of standards implementation that will develop the core principles and standards necessary for teen privacy.

Methodology

This study analyzes privacy issues surrounding the Android mobile app ecosystem, with a focus on mobile apps directed to teenagers.[9] In conducting this study, we aimed to survey the landscape of teen mobile apps for privacy risks and assess how teen data is harvested by the products they use.

TAPP's dataset for this paper is based on a general dataset and a teen dataset.

General Dataset

To create this dataset, we scraped data from the top 200 apps for each genre[10] in the Google Play Store, yielding an initial set of 11,338 apps with accompanying data.[11] We then expanded this dataset to include all apps marked by Google Play as similar[12] to the initial set of 11,338 apps, yielding a total of 53,686 apps, and scraped app data from the Google Play Store to include the entire expanded dataset[13] This scraped data included a list of permissions requested, indicators as to monetization through advertising and in-app purchases, installation counts, links to privacy policies, and in some cases the location of the app publisher.

Teen Dataset

To create this dataset, we identified popular apps (apps which had been installed 20 million or more times) with characteristics likely directed at teenagers. This process yielded a list of 1,322 apps.

To further narrow this sample, we built a multi-factor framework for assessing whether an app was reasonably classified as directed at teens. To construct this framework, we adapted industry standards for marketing to teens, motion picture and software rating guidelines, FTC parameters for assessing the child-directed nature of content for compliance with COPPA, and general knowledge about popular teen products in 2020.[14]

Using this framework as a reference, we manually narrowed our sample to 1,156 teen-directed apps. After identifying these apps, we downloaded the Android application package (APK)[15] of each.[16] Accounting for minor adjustments and download failures, the final list for the teen dataset consisted of 1,144 apps with accompanying APKs.

For each of these datasets, where possible, we assessed multiple privacy dimensions of each app.

- The presence and number of permissions each app requested
- The number of trackers integrated into each app
- The readability of each app's description in the app store
- The presence of each app's privacy policy
- Whether each app monetizes through advertising or in-app purchases

"Teen Directedness"

In addition, we measured the teen dataset and compared it with the general dataset to confirm that our filtering processes produced a list of teen-focused apps. We looked at three points of comparison:

1. Does the genre breakdown change between teen and general datasets? We expected, for example, to see fewer utility apps, business apps, etc. in the teen dataset.
2. Using an appropriate readability scoring formula, is the reading level of the app descriptions on the Google Play Store lower for apps from the teen dataset than for the general dataset? We expect the descriptions of apps targeted at a general audience to score at a higher reading level than the descriptions of apps targeted at teens.
3. Which words predominate in the descriptions? We expected teen-directed apps to use different words in their descriptions as compared with general apps, and we further expected the most common words to be easily associable with teens, their behavior, or their interests.

Genre of Teen Apps

TAPP's teen dataset included popular apps known to include teen users, (e.g., TikTok, Instagram, Facebook, Snapchat), gaming, social media, entertainment, messaging, and file sharing. Notably, gaming apps[17] consisted of 55.8% of our teen dataset but only 30.1% of our general dataset.

Table 1.
Genre Breakdown, Top 10, General Dataset

GENRE	Number of apps
Tools	3558
Education	3188
Health & Fitness	2609
Puzzle Games	2306
Productivity	2130
Lifestyle	1936
Finance	1872
Business	1805
Music & Audio	1712
Entertainment	1677

Table 2.
Genre Breakdown, Top 10, Teen Dataset

GENRE	Number of apps
Action Games	120
Casual Games	88
Photography	79
Video Players & Editors	70
Arcade Games	64
Tools	59
Puzzle Games	57
Sports Games	56
Music & Audio	55
Entertainment	53

Readability of Teen Apps

When the app's descriptions were assessed against the Dale-Chall readability formula,[18] which relies on 3000 "familiar words" that are known by 80% of children in the 5th grade, we observed that the average app description for the teen dataset scored approximately 9, while the average app in the general dataset scored 9.59.

$$0.1579\left(\frac{\text{difficult words}}{\text{words}} \times 100\right) + 0.0496\left(\frac{\text{words}}{\text{sentences}}\right)$$

adjusted Score = Raw Score + 3.6365 (if difficult words more than 5%)

Score	Notes
4.9 or lower	easily understood by an average 4th-grade student or lower
5.0–5.9	easily understood by an average 5th or 6th-grade student
6.0–6.9	easily understood by an average 7th or 8th-grade student
7.0–7.9	easily understood by an average 9th or 10th-grade student
8.0–8.9	easily understood by an average 11th or 12th-grade student
9.0–9.9	easily understood by an average 13th to 15th-grade (college) student
Finance	1872
Business	1805
Music & Audio	1712
Entertainment	1677

Table 3:
Reading Level for Dataset App Descriptions

Dataset	Dale-Chall Score
Teen dataset	9.03
General dataset	9.58
General dataset minus teen dataset	9.59
7.0–7.9	easily understood by an average 9th or 10th-grade student
8.0–8.9	easily understood by an average 11th or 12th-grade student

Word Frequencies, Teen Dataset

We also analyzed word frequency counts in the summaries and descriptions scraped from the Google Play Store for both the teen dataset and the general dataset (with the apps in the teen dataset removed from the general dataset for this comparison), removing punctuation and connective words (e.g., “and,” “the,” “his,” etc.), and consolidating word forms (e.g., “game” includes “gaming,” “games,” “gamer,” etc.). By comparing the frequently occurring words in each dataset, we were able to determine whether the teen dataset predominantly included words directed to teens, or words indicative of their behavior or interests, relative to the general dataset.

The results confirmed the hypothesis that the teen dataset included words associated with teens and their interests. The following tables illustrate this, showing the most common 30 words in each dataset. While many words common to popular apps (such as “game”) are highly ranked in both datasets, in the teen dataset words such as “challenge,” “music,” and “battle” all rank among the most commonly occurring words but are not found among the most common words in the general dataset. In the general dataset, the predominant words indicate a more utilitarian outlook, such as “learn” and “easy.”

Table 4:
30 Most Common Words, Teen Dataset

Word	Count
Game	3998
video	3044
app	2287
play	2182
free	1884
photo	1859
new	1624
use	1509
friend	1455
feature	1329
get	1325
music	1297
make	1282
download	1170
world	1076
best	1030
player	1022
like	962
share	891
fun	848
time	831
create	816
mode	813
one	770
device	765
take	765
support	724
challenge	690
effect	687
battle	644

Table 5:
30 Most Common Words, General Dataset

Word	Count
app	114024
game	108873
use	66293
free	55505
new	53043
play	48548
feature	45705
get	44045
make	39100
time	38804
help	31556
find	30483
video	30392
support	29451
best	28568
device	28241
one	27332
like	27273
world	26529
learn	26033
create	25193
photo	24550
need	24029
phone	23059
download	22376
easy	22025
also	21465
fun	20978
include	20889
share	20141

Monetization: Advertising vs. In-App Purchases

TAPP further examined the number of apps in each dataset that relied on advertising or in-app purchases for monetization. In the mobile app ecosystem, app publishers frequently rely on advertising in the form of contextual advertising[19] or interest-based advertising (IBA, also known as targeted advertising)[20] to monetize their products. Additionally, app publishers may integrate the ability to purchase items, features, and upgrades into their apps (in-app purchases or IAP),[21] We note that our datasets and our program's general experience in the mobile app ecosystem show that many mobile apps employ both methods.

In the teen dataset, almost 83% of apps used advertising to monetize, compared to 51% in the general dataset.

In the teen dataset, 78% of apps contained in-app purchases, compared with less than 50% in the general dataset.

When looking at the genres of gaming apps, games for teens were more likely to have in-app purchases. In the teen dataset, the ratio of apps with in-app purchases to those without was almost 13:1, compared to the general dataset's ratio of 4:1.

Table 6:
Ad-Supported Apps, General Dataset

Advertising Monetization	Number of Apps
Ad supported	27,335
Non-ad supported	26,351

Table 7:
Ad-Supported Apps, Teen Dataset

Advertising Monetization	Number of Apps
Ad supported	948
Non-ad supported	196

Table 8:
In-App Purchase Apps, General Dataset

In-App Purchases Monetization	Number of Apps
In-app purchases	26,599
No in-app purchases	27,087

Table 9:
In-App Purchase Apps, Teen Dataset

In-App Purchases Monetization	Number of Apps
In-app purchases	895
No in-app purchases	249

Table 10:
In-App Purchase Gaming Apps, General Dataset

Gaming Apps	Number of Apps
In-app purchases	12,882
No in-app purchases	3,254

Table 11:
In-App Purchase Gaming Apps, Teen Dataset

Gaming Apps	Number of Apps
In-app purchases	591
No in-app purchases	47

Identifying Third-Party Data Trackers

We used Exodus Privacy's Exodus Core framework[22] to identify third-party trackers in downloaded APKs.[23] Broadly speaking, a tracker is a type of software intended to collect data about user behavior. A tracker can be a "first-party" tracker, created by an app publisher, or a "third-party" tracker, created by an unaffiliated company and integrated by the publisher.

In mobile apps, trackers commonly collect device identifiers, location data, or other characteristics of a mobile device's hardware or software to facilitate data collection for IBA, a common means of monetizing mobile apps and websites.[24]

We disassembled the downloaded APKs from the teen dataset to analyze the "bytecode" of the APKs for the signatures of known trackers and found:

- As seen in Figure 1, the median number of trackers per app was 10.
- As seen in Table 13, the most common tracker was Google AdMob.
- Most trackers are owned by Facebook or Google.
- As seen in Table 14, many of the apps with the highest number of trackers are offered by the Cyprus-based app publisher Outfit7.[25]
- As seen in Table 15, Action games have the largest number of aggregate trackers.
- As seen in Table 16, when gaming apps are taken out of the equation, photography apps have the highest aggregate number of trackers.
- When we examine genres with 15 or more apps in this dataset, word games have the highest tracker count when calculated by median (17), followed by arcade games (14).
- When gaming apps are taken out of the equation, when we examined genres with 15 or more apps in this dataset, we found that social media apps have the highest tracker count when calculated by median (11), followed by photography apps (9).

Figure 1:
Tracker Presence Per App, Teen Dataset

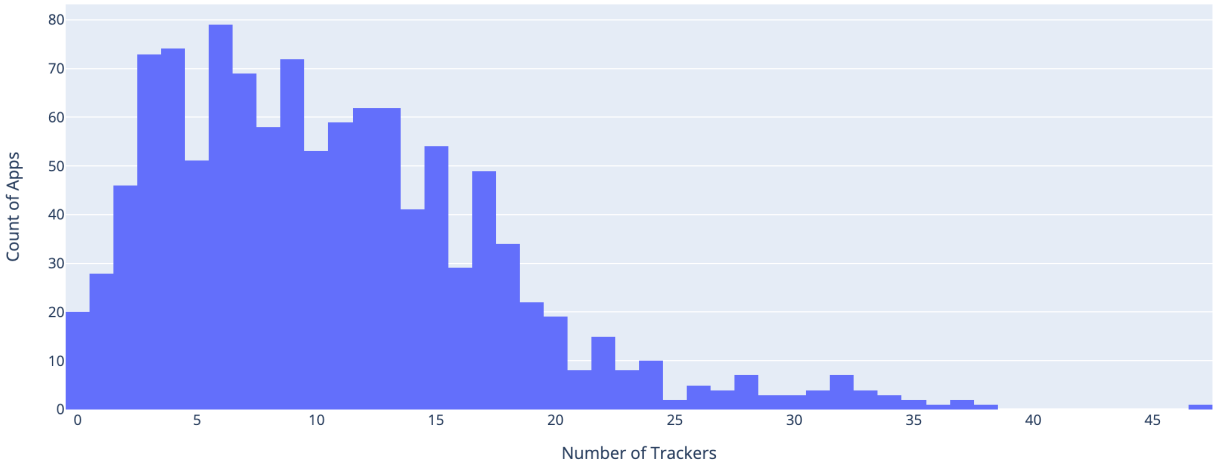


Table 13:
Top 10 Trackers, Teen Dataset

Tracker Name	Number of Apps
Google AdMob	1086
Google Firebase Analytics	981
Facebook Ads	672
Facebook Login	614
Facebook Share	594
Google CrashLytics	580
Facebook Analytics	579
Unity3d Ads	567
Moat (Oracle)	498
AppLovin	402

Table 14:
Apps with Highest Number of Trackers, Teen Dataset

App Name	Number of Trackers
Magic Jigsaw Puzzles	47
My Story: Choose Your Own Path	38
Perfect 365: One Tap Makeover	37
Rodeo Stampede: Sky Zoo Safari	37
Rayman Adventures	36
My Talking Hank	35
Text Me: Text Free, Call Free, Second Phone Number	35
Smurfs' Village	34
Swamp Attack	34
Talking Ben the Dog	34
International Fashion Stylist: Model Design Studio	33
My Talking Tom	33
Talking Tom Cat	33
AXES.io	33
Talking Ginger 2	32
My Talking Tom 2	32
My Talking Tom Friends	32
Talking Angela	32
Talking Tom Candy Run	32
Talking Tom Gold Run	32
Talking Tom Jetski2	32

App Name	Number of Trackers
Talking Tom Hero Dash	31
My Talking Angela	31
Checkers	31
ASKfm-Ask Me Anonymous Questions	30
Talking Ginger	30
Talking Tom and Ben News	30
textPlus: Free Text & Calls	29
Talking Tom Bubble Shooter	29
battle	644

Table 15.
Trackers by Genre, Teen Dataset

Genre	Aggregate Trackers	Number of Apps	Median Trackers
Action Games	1,260	120	9
Casual Games	1,162	88	12
Arcade Games	881	64	14
Puzzle Games	779	57	13
Photography	661	79	9
Sports	644	56	11
Entertainment	567	53	9
Music & Audio	537	55	8
Video Players & Editors	535	70	7
Racing Games	518	48	10

Table 16.
Trackers by Genre, Games Removed, Teen Dataset

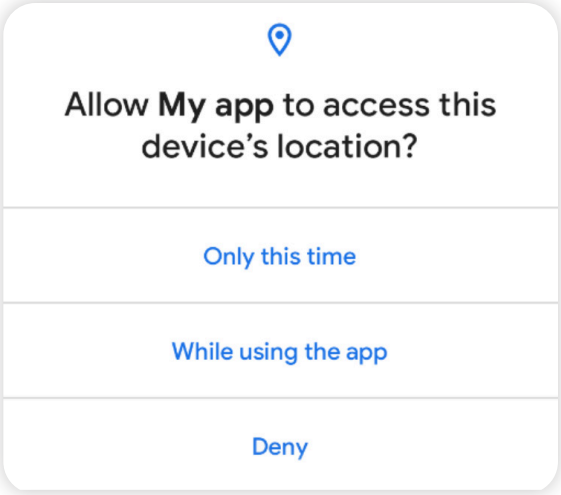
Genre	Aggregate Trackers	Number of Apps	Median Trackers
Trackers	1,162	88	12
Photography	661	79	9
Entertainment	567	53	9
Music & Audio	537	55	8
Video Players & Editors	535	70	7
Tools	449	59	6
Social	390	31	11
Communication	245	37	6
Personalization	191	21	8
Health & Fitness	169	22	8
Shopping	102	11	11

Analyzing App Permissions Requests

Mobile apps can request permission to access certain device features such as a Global Positioning System (GPS) location, microphone, and/or camera. Permissions requests typically come in the form of a pop-up box that requires the user to either enable or disable the request, while other permissions are enabled automatically in the app, such as permissions for internet access (see Figure 2).[26]

Google states that "the purpose of a permission is to protect the privacy of an Android user."[27] Google Play store policies indicate that apps should not ask permission to access something that they do not need to function (e.g., an e-reading app should not need to request a location permission to function).

Figure 2:
Example – Google App Permission Request



To conduct our analysis of permissions requests, we relied on both public data scraped from the Google Play Store and data that we obtained from each app's manifest[28] as a result of our static analysis. Wherever possible, we relied on the manifest permissions list that we analyzed in each app's APK. However, to obtain equivalent data when comparing general and teen datasets, we used permissions data scraped from the Google Play Store. This is because the Google Play Store data and the information contained in an app's manifests may differ.

Based on the data listed in the Google Play Store, apps in the teen dataset requested a median of 11 permissions per app compared to 10 permissions per app in the general dataset.

In our static analysis, conducted of the apps in the teen dataset, we found the median number of permissions requested in the teen dataset was 8 (Figure 3).[29]

282 apps requested 6-7 permissions, the mode of the teen dataset (Figure 3).

5 apps requested more than 50 permissions each, with 2 of those apps requesting over 100 permissions each (Figure 3).

Apps from the teen dataset in the "Tools" genre were found to have the largest number of aggregate permissions requests, followed by communication apps (Table 21).

Dangerous Permissions Requests

The Google Play Store categorizes permissions requests into three categories: normal, signature, and dangerous. Normal permissions requests pose little threat to user privacy, whereas dangerous permissions "involve the user's privacy information or could potentially affect the user's stored data or the operation of other apps.[30]" For example, accessing a device's fine location or camera would be considered dangerous permissions requests.

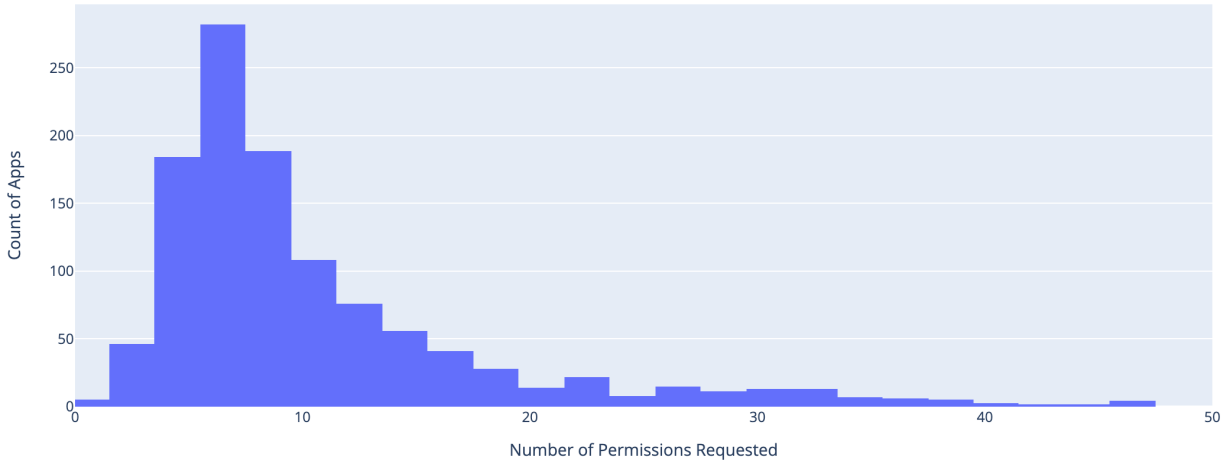
When examining publicly scraped data from the Google Play Store, we found that there was a median of 5 dangerous permissions requested for apps in the general dataset compared to a median of 6 dangerous permissions requested in the teen dataset.

Looking at permissions requests data from the teen dataset's app manifests, we identified the top 10 dangerous permissions requested across teen-directed apps as well as the top 5 trackers associated with apps requesting those dangerous permissions (Tables 19 & 20).

Though the permissions requests are visible to the user, the trackers themselves are often not. When comparing which trackers appeared with which permissions a specific app requested, adjusting for how many times a tracker appeared overall in the teen dataset, we identified the top 5 trackers associated with each common dangerous permission request.

Echoing the earlier tracker analysis, most trackers identified as frequently co-occurring with dangerous permissions are controlled by Facebook and Google.

Figure 3:
Permissions Requested per App, Teen Dataset



Top 10 Requested Permissions, Teen Dataset

Permission Name	Function	Protection Level	Number of Apps
INTERNET	Allows applications to open network sockets	Normal	1139
ACCESS_NETWORK_STATE	Allows applications to access information about networks	Normal	1136
WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.	Normal	1072
WRITE_EXTERNAL_STORAGE	Allows applications to write to external storage	Dangerous	851
ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks	Normal	832
VIBRATE	Allows access to the vibrator.	Normal	701
READ_EXTERNAL_STORAGE	Allows applications to read from external storage. Any app that declares the WRITE_EXTERNAL_STORAGE permission is implicitly granted this permission.	Dangerous	697
RECEIVE_BOOT_COMPLETED	Allows applications to receive the Intent.ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.	Normal	485
FOREGROUND_SERVICE	Allows a regular application to use Service.startForeground.	Normal	359
CAMERA	Required to be able to access the camera device.	Dangerous	294

Table 18:
Apps Requesting the Greatest Number of Permissions, Teen Dataset

Word	Count
Parallel Space – Multiple accounts & Two face	102
Parallel Space Lite – Dual App	102
Samsung Smart Switch Mobile	66
EasyShare – Ultrafast File Transfer, Free & No Ads	60
GO Launcher - 3D parallax Themes & HD Wallpapers	52
Truecaller: Caller ID, block fraud & scam calls	47
Signal Private Messenger	47
Messenger for SMS	46
WeChat	46
Free phone calls, free texting SMS on free number	45
TextNow: Free Texting & Calling App	43
AirDroid: Remote access & File	43
UC Browser- Free & Fast Video Downloader, News App	41
C launcher:DIY themes,hide apps,wallpapers,2020	40
KakaoTalk: Free Calls & Text	40
GO Security—AntiVirus, AppLock, Booster	39
Mi Browser Pro - Video Download, Free, Fast&Secure	39
WhatsApp Messenger	39
OK	39
Skype - free IM & video calls	38
APUS Launcher - 3d wallpaper&Themes,Hide apps	37
Safe Security - Antivirus, Booster, Phone Cleaner	37
UC Mini-Download Video Status & Movies	37
Uplive - Live Video Streaming App	36
Facebook	36
SHAREit - Transfer & Share	36
Mi Remote controller - for TV, STB, AC and more	35
BOTIM - Unblocked Video Call and Voice Cal	35
Eyecon: Caller ID, Calls and Phone Contacts	34
AppLock	34

As seen above, we identified 5 apps requested over 50 permissions each, with 2 of those apps requesting over 100 permissions each.

Table 19:
Top 10 Requested Dangerous Permissions, Teen Dataset

Permission Name	Function	Number of Apps
WRITE_EXTERNAL_STORAGE	Allows app to write to external storage	851
READ_EXTERNAL_STORAGE	Allows app to read from external storage. Any app that declares the WRITE_EXTERNAL_STORAGE permission is implicitly granted this permission.	697
CAMERA	Required to be able to access the camera device.	294
RECORD_AUDIO	Allows app to record audio. (Enables the device microphone)	265
READ_PHONE_STATE	Allows read-only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device	281
ACCESS_COARSE_LOCATION	Allows app to access approximate location.	225
GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.	216
ACCESS_FINE_LOCATION	Allows app to access precise location	201
READ_CONTACTS	Allows app to read the user's contacts data.	128
WRITE_CONTACTS	Allows app to write the user's contacts data.	50

Table 20:
Top 5 Trackers Associated with Dangerous Permissions, Teen Dataset

Permission Name	Associated Trackers
WRITE_EXTERNAL_STORAGE	Google Crashlytics Facebook Login Facebook Share Facebook Analytics Moat
READ_EXTERNAL_STORAGE	Google Crashlytics Facebook Login Facebook Share Facebook Analytics Moat
CAMERA	Facebook Share Facebook Login Google Crashlytics Facebook Analytics AppsFlyer
RECORD_AUDIO	Facebook Share Facebook Login Facebook Analytics AppsFlyer Google Crashlytics
ACCESS_COARSE_LOCATION	Facebook Share Facebook Login Facebook Analytics Google Grashlytics Twitter MoPub
ACCESS_FINE_LOCATION	Facebook Login Facebook Share Facebook Analytics Google Analytics Facebook Places
READ_CONTACTS	Google AdMob Google Firebase Analytics Facebook Ads Facebook Login Facebook Share
READ_PHONE_STATE	Facebook Login Facebook Analytics Facebook Share Google Crashlytics Facebook Places
GET_ACCOUNTS	Facebook Login Facebook Share Google Crashlytics Facebook Analytics Facebook Places
WRITE_CONTACTS	Google AdMob Google Firebase Analytics Facebook Ads Facebook Login Facebook Share

Table 21:
Top 10 Genres Requesting Most Permissions, Teen Dataset

1. Tools
2. Communication
3. Photography
4. Video Players & Editors
5. Action Games
6. Social
7. Music & Audio
8. Casual Games
9. Entertainment
10. Personalization

Table 22:
Top 10 Genres by Number of Permissions Requested, Teen Dataset

App Genre	Aggregate Permissions	Number of Apps	Median Permissions
Tools	1211	59	17
Communication	1090	37	32
Photography	925	79	10
Video Players & Editors	853	70	10
Action Games	830	120	6
Social	782	31	23
Music & Audio	743	55	13
Casual Games	586	88	6
Entertainment	584	53	9
Personalization	494	21	18

Table 23:
Top 10 per Genre by Number of Permissions Requested, Games Removed, Teen Dataset

App Genre	Aggregate Permissions	Number of Apps	Median Permissions
Tools	1211	59	17
Communication	1090	37	32
Photography	925	79	10
Video Players & Editors	853	70	10
Social	782	31	23
Music & Audio	743	55	13
Entertainment	584	53	9
Personalization	494	21	18
Health & Fitness	305	22	11
Productivity	217	15	15

Apps from our teen dataset in the "Tools" genre have the largest number of aggregate permissions, followed by communication apps. When we examine genres with 15 or more apps in our dataset, we find that communications apps request the greatest median number of permissions, followed by social media apps.

Looking at the Global App Publisher Landscape

Starting with the information provided in each Play Store profile, TAPP correlated each app in the teen dataset to the country where its developer is based[31] to identify the countries[32] with the greatest number of apps in the dataset and whose correlating apps contained the most trackers. Notably, approximately 9% of apps in the teen dataset did not provide any clear address information for their developers, which required us to conduct independent research to identify these developers' home countries.

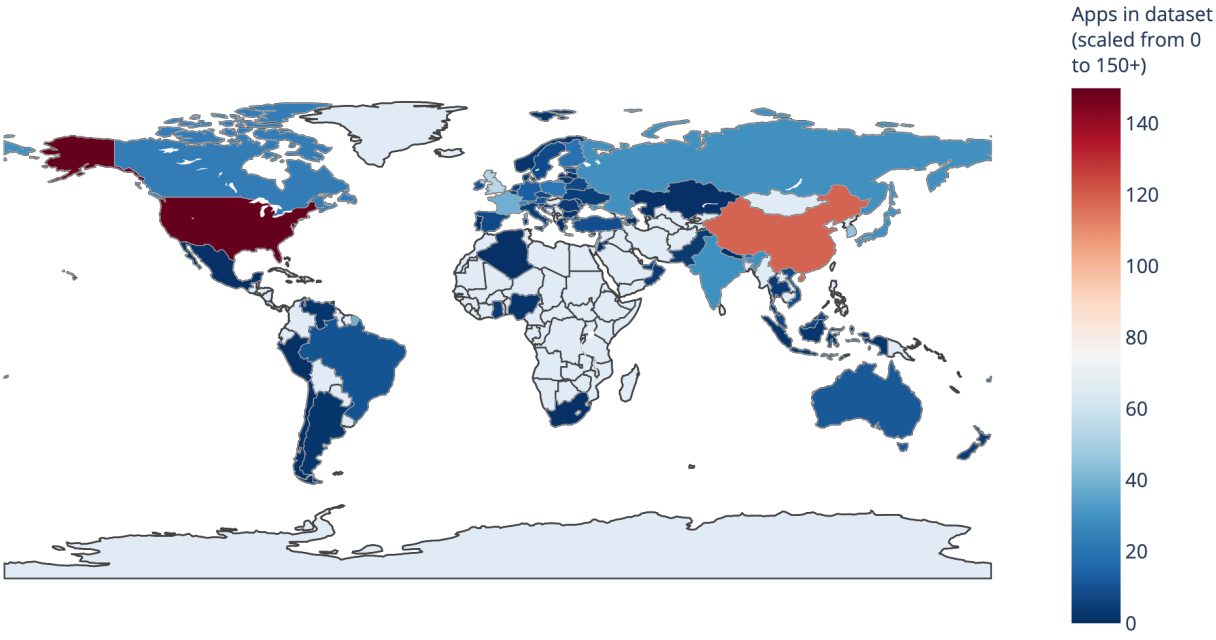
Using this information, we identified:

- Countries with app publishers with the highest tracker count (Table 25).
- The countries with apps that requested the most permissions (Table 26).
- In-app purchase percentages for top app publisher countries (Figure 5).

Table 24:
Countries with Greatest Number of Apps, Teen Dataset

Country	Number of Apps
United States	342
China	119
United Kingdom	54
South Korea	46
Singapore	43
France	39
Cyprus	37
Israel	36
Russia	30
India	29

Figure 4:
Heat Map of Countries with Most Apps, Teen Dataset



On the next page, Table 25 illustrates the median number of trackers per app associated with each country. To provide a more objective look at the overall privacy impact of each country's app publishers, we set a threshold for each country excluding any with fewer than 30 associated apps. We further provide in Table 26 the countries with the most permissions requested per app from the teen dataset.

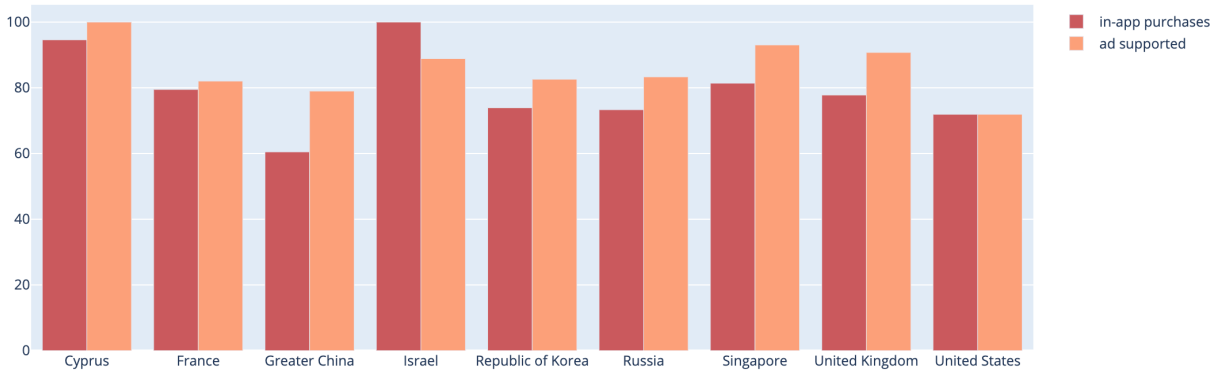
Table 25:
Countries with Most Trackers per App, Teen Dataset

Country	Median Trackers
Cyprus	28
Israel	17
France	13
United Kingdom	11
China	10
United States	9
Singapore	9
Russia	7
South Korea	6

Table 26:
Countries with Most Permissions Requested per App, Teen Dataset

Country	Median Trackers
China	18
South Korea	15.5
France	15
United States	14
Singapore	11
Russia	10
Israel	10
United Kingdom	9
Cyprus	9

Figure 5:
In-App Purchases Percentages, Teen Dataset



Here, in Figure 5 above, we observe that a high percentage of each country's app products monetize through in-app purchases.[33] We speculate that app developers aim to maximize their monetization through a combination of data collection for advertising and in-app purchases, especially if they offer a product that achieves a high installation count.

Conclusion

This study demonstrates an unchecked ecosystem of data collection for a uniquely vulnerable audience. Teen data privacy is a complex topic that does not belong in the same conversations as data privacy regulation for children. As the data show, teens are voracious users of digital media platforms, and their quest for greater engagement threatens the safety of their personal data.

We look forward to more opportunities to continue this research and encourage companies interested in joining the efforts of the TeenAge Privacy Program to reach out and contact us at **TAPP@bbbnp.org**.

---

[1] See generally Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. See also Federal Trade Commission, Children's Online Privacy Protection Rule ("COPPA"), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (last visited Sept. 16, 2020).

[2] See Marketing Charts, US Population Distribution, by Age Group and Gender (July 1, 2019), https://www.marketingcharts.com/charts/us-population-distribution-by-age-and-gender-in-2019/attachment/censusbureau-us-population-distribution-by-age-group-and-gender-july2020, noting individuals between 12-17 year old represent 7.6 percent of the total population.

[3] J. Clement, U.S. mobile device owner monthly app download rate 2018, by age group, Statista, (Dec. 6, 2019), https://www.statista.com/statistics/243794/us-adult-cell-phone-owners-who-have-downloaded-apps-by-age-group/.

[4] Rideout, V., and Robb, M.B., Social Media, Social Life: Teens Reveal Their Experiences, Common Sense Media (2018), https://www.commonsensemedia.org/sites/default/files/uploads/research/2018-social-media-social-life-executive-summary-web.pdf.

[5] Id.

[6] Id.

[7] See generally, Congress.gov, H.R.5573 - PROTECT Kids Act, https://www.congress.gov/bill/116th-congress/house-bill/5573?s=1&r=1 (last visited Oct. 22, 2020). Markey.senate.gov, SENATORS MARKEY AND BLUMENTHAL INTRODUCE FIRST-OF-ITS-KIND LEGISLATION TO PROTECT CHILDREN ONLINE FROM HARMFUL CONTENT, DESIGN FEATURES (March 5, 2020),https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-introduce-first-of-its-kind-legislation-to-protect-children-online-from-harmful-content-designfeatures_#:~:text=and%20Senator%20Richard%20Blumenthal%20(D,and%20Safety%20(KIDS)%20Act.&text=%E2%80%9CBig%20Tech%20has%20designed%20their,purchases%2C%E2%80%9D%20said%20-Senator%20Blumenthal.

[8] Pew Research Center, Teens, Social Media, and Privacy (May 21, 2013), https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/.

[9] We note that due to our research methodology it was easier to narrow the focus of this paper to the Android mobile app ecosystem. We do not intend to provide commentary on the privacy practices of Apple and Google in relation to one another. Nothing in this report is intended or should be construed to be an endorsement or critique of a company's policies or practices.

[10] See generally Google Play Store, Top Charts, https://play.google.com/store/apps/top?hl=en_US (last visited Sept. 9, 2020). Genres can be access by clicking "categories" option. We note that genres include, but are not limited to, the following: 'Dating,' 'Education,' 'Entertainment," ''Finance,' etc.

[11] See generally Google-play-scraper, https://github.com/facundoolano/google-play-scraper/ (last visited Sept. 8, 2020).

[12] TAPP notes that a similar app is an app linked on the sidebar of a Google Play Store app page under "similar."

[13] This figure is the final number of apps for our general dataset after some errors were removed.

[14] The Digital Advertising Accountability Program relied on the following framework to assess the teen-directed nature of apps. (1) The subject matter, including childish pranks, rites of passage, youth romance, fashion, beauty, sports, performing arts, or mental health. (a) Subject matter appealing primarily to children, such as basic spelling or counting, elementary school arithmetic, most coloring books, and low-vocabulary apps, is not considered to be directed at teenagers. (b) Subject matter chiefly of interest to or appropriate only for adults, such as business, finance, gambling, or pornography is not considered to be directed at teenagers (i) Notwithstanding factor (1) (b) of these guidelines, business or utility-oriented apps that provide features of strong interest to teenagers, such as file sharing or video downloading, may be considered as directed to teenagers, even though such apps may appear to be targeted primarily to adults. (2) Visual content, including settings appealing to teenagers such as skate parks, zoos, summer camps, or teen clubs. (a) Visual depictions targeted at teenagers may include depictions of violence, suggestive themes, crude humor, minimal blood, and some strong language. (b) Visual content appealing to young children, such as brightly colored animated creatures, fairy tale settings, or other images or activities associated with young children, is not considered to be directed to teenagers. (c) Visual content chiefly of interest to or appropriate only for adults, such as intense violence, blood and gore, and sexual content is not considered to be directed to teenagers. (3) The use of teenager-oriented characters, activities, or incentives, particularly involving characters under the age of 25. (4) The kind of music or other audio content. (5) Models appearing to be under the age of 25. (6) The presence of celebrities who appeal to teenagers. (7) Language or other characteristics of the app. (8) Whether advertising that promotes or appears on the app is directed to teenagers. (9) Notwithstanding the prior sections of these guidelines, apps which are known to be popular among teenage users may be considered as directed to teenagers, even though such apps may appear to be targeted primarily to other users. We note that this framework was influenced by the Entertainment Software Ratings Board ratings, factors the FTC has established for examining, the child-directed nature of content, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0, standards for ratings set by the Motion Picture Association of America, https://www.filmratings.com/downloads/rating_rules.pdf, and the EU's Responsible Marketing Pact for avoiding the exposure of minors to advertising for alcoholic beverages, https://www.filmratings.com/downloads/rating_rules.pdf. See generally Entertainment Software Ratings Board, Ratings, https://www.esrb.org/ratings/ (last visited Sept. 8, 2020), Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, § D.1., https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (last visited Sept. 8, 2020). FTC v. TinyCo, FTC Matter 132 3209 (Sept. 2014), https://www.ftc.gov/system/files/documents/cases/140916tinycocmpt.pdf. Motion Picture Association, Inc., Classification and Rating Rules (July 24, 2020), https://www.filmratings.com/downloads/rating_rules.pdf. Responsible Marketing Pact, Content of Ads, https://the-rmp.eu/content/ (last visited Sept. 8, 2020).

[15] Android Developers, Application Fundamentals, https://developer.android.com/guide/components/fundamentals(last visited Sept. 29, 2020) ("Android apps can be written using Kotlin, Java, and C++ languages. The Android SDK tools compile your code along with any data and resource files into an APK, an Android package, which is an archive file with an .apk suffix. One APK file contains all the contents of an Android app and is the file that Android-powered devices use to install the app.").

[16] Gplaycli, https://github.com/matlink/gplaycli (last visited Sept. 8, 2020).

[17] We note that gaming apps constitute multiple genres, e.g. 'Casual,' 'Educational,' 'Music'

[18] Brian Scott, The Dale-Chall 3,000 Word List for Readability Formulas, https://www.readabilityformulas.com/articles/dale-chall-readability-word-list.php (last visited Sept. 9, 2020). See also Readability Formulas, The New Dale-Chall Readability Formula, https://readabilityformulas.com/new-dale-chall-readability-formula.php (last visited Sept. 9 2020).

[19] eMarketer, Mobile Trends 2020: 10 Trends to Monitor As 5G Ramps Up and Privacy Battles Loom, https://on.emarketer.com/rs/867-SLG-901/images/Branch-Mobile%20Trends%202020%20Report%20Sponsorship.pdf (last visited Sept. 16, 2020) ("...[T]here is a resurgence of interest in sophisticated contextual advertising, i.e., using the context of the app or web page to infer the interests of the user instead of gathering historical behavior to gauge those interests.").

[20] See generally Digital Advertising Alliance, Consumer Assistance, WebChoices and AppChoices,https://youradchoices.com/choices-faq#jr02 (last visited Sept. 16, 2020) ("When a user visits a website or uses an app that works with an advertising network or other online advertising companies, these advertising companies gather information about the user's browser or device in order to tell when that same user browser or device visits other websites or apps within the same network – even if these content offerings are run by different companies or have different web addresses or brands. Over time, the information gathered about the browser or device may help predict the user's likely interest in particular categories of ads: for example, users who frequently visit baseball-related websites might receive more ads for the "baseball/sports enthusiast" category, or users who engage with automobile review apps might receive more ads for the particular models of cars that interest them. This inferred interest category is used to provide advertising relevant to the category to a particularly browser or device.").

[21] Google, Make in-app purchases of Android apps, https://support.google.com/googleplay/answer/1061913?hl=en (last visited Sept. 9, 2020) ("With some apps, you can buy additional content or services within the app. We call these "in-app purchases." Here are some examples of in-app purchases: A sword that gives you more power in a game...A key that unlocks more features of a free app...Virtual currency that can be used for purchases."). Apple, Buy additional app features with in-app purchases and subscriptions, https://support.apple.com/en-us/HT202023 (last visited Sept. 9, 2020).

[22] See generally Exodus Privacy, Who we are, https://exodus-privacy.eu.org/en/page/who/ (last visited Sept. 8, 2020). See also Exodus-Privacy, https://github.com/Exodus-Privacy/exodus-core (last visited Sept.8, 2020). TAPP notes that the Exodus Core set of frameworks uses "dexdump," a standard Android platform tool, to disassemble the APK. This tool looks at the app manifest to determine permissions requested, then looks over the bytecode for the signatures of known trackers previously identified by Exodus. Exodus Privacy, Trackers https://reports.exodus-privacy.eu.org/en/trackers/ (Sept 8. 2020). See generally Google Git, Dexdump, https://android.googlesource.com/platform/dalvik/+/09239e3/dexdump (last visited Sept. 8, 2020). Android Developers, App Manifest Overview, https://developer.android.com/guide/topics/manifest/manifest-intro (last visited Sept. 8, 2020). Android Developers, Dalvik bytecode, https://source.android.com/devices/tech/dalvik/dalvik-bytecode (last visited Sept. 8, 2020). See generally Wikipedia, Bytecode, https://en.wikipedia.org/wiki/Bytecode (last visited Sept. 8, 2020) ("Bytecode, also termed portable code or p-code, is a form of instruction set designed for efficient execution by a software interpreter. Unlike human-readable source code, bytecodes are compact numeric codes, constants, and references (normally numeric addresses) that encode the result of compiler parsing and performing semantic analysis of things like type, scope, and nesting depths of program objects.").

[23] Exodus Privacy, What Exodus Privacy Does, https://exodus-privacy.eu.org/en/page/what/ (last visited Sept. 8, 2020) ("A tracker is a piece of software meant to collect data about you or what you do."). Gunes Acar, Online Tracking Technologies and Web Privacy (May 2017), https://www.esat.kuleuven.be/cosic/publications/thesis-289.pdf ("Android apps and third-parties can access common identifiers present on the smartphone, such as MAC address, Google Advertising ID or IMEI number."). See generally Interactive Advertising Bureau, Mobile Identity Guide for Marketers (June 2017), https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf.

[24] See generally Digital Advertising Alliance, DAA Self-Regulatory Principles, https://digitaladvertisingalliance.org/principles (last visited Sept. 14, 2020). See also OBA Principles Summary at 2, ("The Principles apply to online behavioral advertising, defined as the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors.") See generally Mobile Guidance. TAPP notes that the DAA's Self Regulatory Principles can be located here: https://digitaladvertisingalliance.org/principles.

[25] See generally Outfit7, Outfit7, https://outfit7.com (last visited Sept. 14, 2020).

[26] Android Developers, Permissions Overview, https://developer.android.com/guide/topics/permissions/overview (last visited Sept. 16, 2020).

[27] Id.

[28] Android Developers, App Manifest Overview, https://developer.android.com/guide/topics/manifest/manifest-intro (last visited Sept. 16, 2020) ("Every app project must have an AndroidManifest.xml file (with precisely that name) at the root of the project source set. The manifest file describes essential information about your app to the Android build tools, the Android operating system, and Google Play.").

[29] We note that this discrepancy is likely the result of the way the Google Play Store tracks permissions. Permissions requests listed in old versions of apps may still be listed on the Google Play Store, even if the current version does not request those permissions. Consequently, data from the Google Play Store version will tend to show that an app has a higher permissions requests count, versus the permissions requests count that results from a static analysis of a downloaded APK.

[30] Android Developers, Permissions overview, https://developer.android.com/guide/topics/permissions/overview (last visited Sept. 17, 2020). We do not analyze signature permissions requests as a distinct category in this paper.

[31] Not all of the publicly scraped data for app store pages provided an app publisher location. Of the 1144 apps in the teen dataset, all but 99 could be matched to their developer's countries based on keyword matches to their provided address. The 99 remaining either had blank addresses or provided so little information that they could not readily be matched to a country. Of those 99, 87 could be matched with countries based on investigating the developers to identify their likely locations. 12 apps remain unmatched.

[32] Chinese Taipei and Hong Kong are included within "Greater China." See generally Asia-Pacific Economic Cooperation, https://www.apec.org/ (last visited Sept. 9, 2020).

[33] Here, we again used a threshold of countries with at least 30 app products to calculate which countries had a set of apps with the highest percentage of in-app purchases.