Me2B ALLIANCE

Spotlight Report #1

Me2B Alliance Product Testing Report:
School Mobile Apps Student Data Sharing Behavior

Research Performed by Zach Edwards and Lisa LeVasseur
Written by Lisa LeVasseur, Zach Edwards, Karina Alexanyan
Contributors: Eve Maler, Shaun Spalding

May 4, 2021

1 ABSTRACT

The Me2B Alliance Product Testing team audited and analyzed a random sample of 73 mobile applications used by 38 schools in 14 states across the U.S., covering at least a half a million people (students, their families, educators, etc.) who use those apps. The audit methodology mainly consisted of examining data flow from the apps to external third-party vendors, by evaluating the SDKs included in each app. This report details and summarizes the audit findings.

The analysis found that the majority (60%) of school apps were sending student data to a variety of third parties. These included advertising platforms such as Google, to which about half (49%) of the apps were sending student data, as well as Facebook (14%). On average, each app sent data to 10.6 third-party data channels.

Two thirds (67%) of the public schools in the sample were sending data from apps to third parties. This finding is particularly troubling since public schools most likely utilized public funding to develop or outsource the apps – meaning that taxpayers most likely paid to fund apps that are sending student data to online advertising platforms. Moreover, public schools were more likely to send student data to third parties than private schools (67% vs. 57% of private school apps).

Another disturbing public-school finding: 18% of public-school apps sent data to what the Me2B Alliance deems *very high-risk* third parties – i.e., entities that further share data with possibly hundreds or thousands of networked entities. Zero private school apps in this study sent data to any *very high-risk* third parties.

The research also showed that Android apps are three times more likely than iOS apps to be sending data to third parties, and are much more likely to be sending data to *high* or *very high-risk* third parties: 91% of Android apps send data to *high-risk* third parties compared to only 26% of iOS apps, and 20% of Android apps sent data to *very high-risk* third parties, compared to 2.6% of iOS apps.

Additionally, while not examined in detail, the analysis confirmed that the data sent to third parties typically

included unique identifiers (through Mobile Advertising Identifiers, or MAIDs), thus enabling profile building for students – including those under the age of 13 – by third-party advertising platforms. Apple's new AppTrackingTransparency framework[1] and changes to its incumbent IDFA (Apple's mobile Identifier For Advertisers) system reduce the risk of the profile building that's described in this research. This change increases the "respectfulness gap" between iOS and Android apps, although it may not fully remove the risk of profile building.

Also troubling is that the analysis found data being sent to third parties as soon as the app is opened by the user – even if they are not signed into the app. In most apps, third-party data channels initiated initial data transfers and ID syncs as soon as the app is loaded.

The researchers estimate that upwards of 95% of the third-party data channels are active even when the user isn't signed in[2].

Our research did *not* include a deeper look into the third parties to understand whether or not these entities were taking appropriate care of student data, in particular for children under the age of 13, important in light of the Children's Online Privacy Protection Act of 1998 (COPPA), which outlines requirements for the handling of personal information for children under the age of 13. 85% of the schools included in this analysis have students under the age of 13.

Further, neither the Google Play Store nor the Apple App Store include details on which third parties are receiving data, leaving users no practical way to understand *to whom* their data is going, which may well be the most important piece of information for people to make informed decisions about app usage.

Professional organizations appeared to have created 99% of the apps and only 1 app appeared to be "home grown" based on developer metadata, but the latter could have been developed by professional organizations or contractors who used the school's iOS developer account to upload the apps. 77 percent of the apps were built by six educational app companies.

The analysis also examined average app ages to determine if privacy practices and notifications were current. The average age of apps in the study was 11.6 months – apps were being updated roughly annually. It should be noted that at the time of this research, 75% of the iOS apps in the study had not been updated since December 2020 - when the Apple App Store's new Privacy Labels began to be required – and therefore didn't include a Privacy Label.

Finally, in the course of the research it was observed that three schools (8% of those studied) offered only iOS apps. Given the price difference between Apple and Android devices, there is a small concern that this practice could leave some families behind, possibly exacerbating the "digital divide".

This research is intended to illuminate the pervasiveness of data sharing with *high-risk* entities in order to effect change in app development practices, app notification practices, and ultimately to provide policy

---

[1] "Apple Launches the Post-IDFA World to the Dismay of Advertisers", *Venture Beat,* April 21, 2021, Dean Takahashi, https://venturebeat.com/2021/04/21/apple-launches-the-post-idfa-world-to-the-dismay-of-advertisers/

[2] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *New York Times,* December 10, 2018, Jennifer Valentino-DeVries, et al. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

makers with information to ensure the right funding support and protections are in place to protect our most vulnerable citizens – our children.

The key takeaways are:

- There is an unacceptable amount of student data sharing with third parties – particularly advertisers and analytics platforms – in school apps.
- School apps – whether iOS or Android, public or private schools – should not include third-party data channels.
- iOS apps were found to be safer than Android apps, and with ongoing improvements the "privacy gap" between iOS and Android apps is expected to widen unless Google makes some changes.
- People still have too little information about which third parties they're sharing data with, and the app stores (Apple and Google Play) must make this information clearer.

2 INTRODUCTION

The Me2B Alliance is a Standard Development Organization (SDO) establishing the Me2B Respectful Tech Specification, to ensure that technology treats people right.

In addition to supporting the creation of the specification, the Me2B Alliance (Me2BA) performs independent product testing using the principles in the specification in order to illuminate risks and harms in the behavior of connected technology. This testing lets people ("Me-s") make safer technology choices, and "B-s" (makers of technology) build safer, more respectful technology. From the Alliance's product testing experience, it is often the case that makers of technology may be unaware of some of the downstream behavior of integrated technologies or partners. In short, technology is increasingly complicated and difficult to know with specificity.

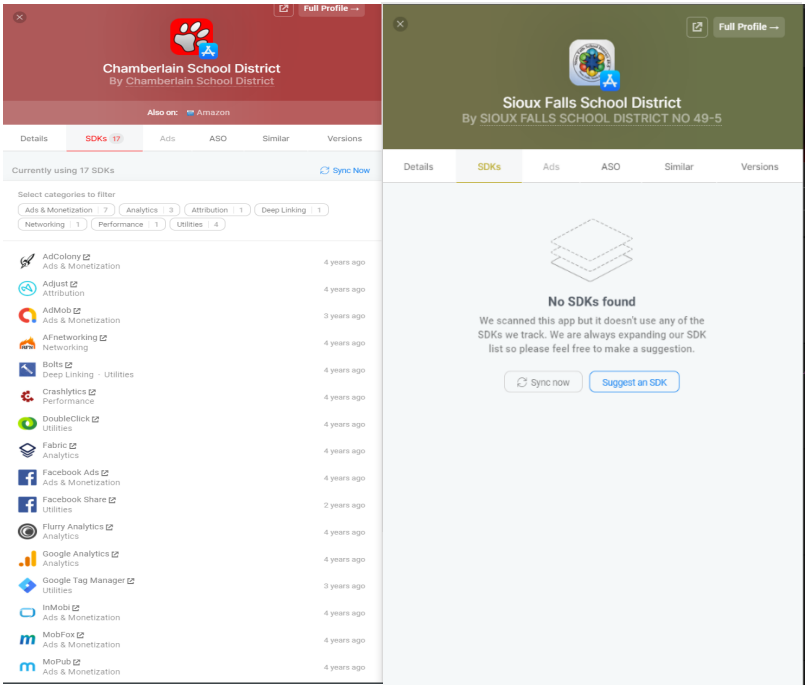
We recognize that school administrators and decision-makers for school app choices may not be technical experts and may rely on the expertise of software suppliers. Our intention in publishing this research is to drive awareness across the spectrum of students, parents, teachers, administrators, local governments, policy makers, and makers of educational software, for a safer society. As a 501c3 non-profit in the U.S., we are available to assist any concerned stakeholder in navigating what's happening "under the hood", in order to keep everyone – and especially our children – safe in the digital world.

3 METHODOLOGY

The research focuses on the data sharing practices of education apps that were associated with a school or school district. This study included a random sampling of 73 apps – usually an Android and Apple pair (except for three schools which used only Apple apps) – from 38 public and private schools in 14 states across the U.S., including California, Hawaii, Kansas, Maine, Massachusetts, Minnesota, Mississippi, Nebraska, Oregon, South Dakota, Tennessee, Vermont, Virginia, and Washington.

This research reflects a small subset of the tests included in the *Me2B Respectful Tech Specification*. This subset is part of the *Data Integrity Tests*, which focus on the data flow happening "under the hood" of technology.

For our research, the Alliance utilized tools from AppFigures.com, an analytics firm which provides a database of software development kits (SDKs), permissions, and other data about mobile apps across all the major app stores. Figure 1 below provides an example of the SDK information provided by AppFigures.



Source: Appfigures.com

Figure 1: Sample SDK information used in the research showing an app with multiple SDKs and an app with no SDKs.

3.1 SDK Analysis

Most mobile apps are built with SDKs, which provide app developers with pre-packaged functional modules of code, along with the potential of creating persistent data channels directly back to the third-party developer of the SDK. SDKs almost always start running "behind the scenes" as soon as a user opens a mobile app – without the express consent of the user. These SDK providers use this data for a variety of reasons, from performing vital app functions to advertising, analytics and other monetization purposes.

In Me2B vernacular, third-party SDKs are "Hidden B2B Affiliates", i.e., they are suppliers to the app developer, with whom the user doesn't have a direct relationship, but the app (and the app developer) does. The user has a Me2B relationship with the app developer, as memorialized by the acceptance of the app's Terms of Service or Terms of Use. The user also has a Me2P (Me-2-Product) relationship with the app itself. The Me2P relationship is the ongoing relationship between the user and the technology. Not only does the user not have a direct (Me2B) relationship with the SDK providers, app users typically have no way to even know who the Hidden B2B Affiliates are. Users are unwittingly in Me2P relationships with SDKs.

A crucial part of the research methodology was to study both the number and the type of SDKs included in the mobile apps. In particular, SDKs were categorized based on their potential for harm (i.e., abuse or exploitation of information). AppFigures has a list of 25 SDK categories, and the heuristic for category assignment is sometimes unclear[3]. The original 25 categories used by AppFigures were condensed into three categories: ***Utility***, ***Analytics***, and ***Advertising*** (or combinations thereof). Each SDK was classified into one or more of these three categories based on the nature of the underlying business model of the SDKs in the category. If, for example, at least one of the SDKs listed in the original AppFigures category performs a function related to advertising, the group was designated as ***Advertising.***

Additionally, one of three risk attributions, ***medium***, ***high***, and ***very high***, was assigned for each category based on the prevailing behavior of the SDKs in the category, as well as the potential harm caused by an SDK's abuse or exploitation of information.

Utility SDKs perform functions necessary to deliver expected behavior to the app user. In our analysis, these SDKs are lower risk. But given the potential for information exploitation or abuse in virtually any SDK – particularly given the age of the app users in this analysis – none of the Utility SDKs can be considered without potential for harm***.*** This category of SDKs is designated as ***medium risk*****.**

Analytics SDKs collect behavioral analytics to be used by the app developer (first party), or by the SDK developer (third party), or passed along to other third parties. Analytics SDKs are designated as ***high-risk*** because they often either uniquely identify (fingerprint) individuals or include other potential for data exploitation. Many analytics SDKs either directly support advertising networks or have advertising network partners and their data should be assumed to be associated with online advertising.

Advertising SDKs explicitly perform digital advertising functions, and include several of the AppFigures designations, such as Attribution, Deep Linking, Engagement, Insights, Payments and Location, among others. All Advertising SDKs are designated as ***high-risk*** – particularly in this analysis of educational apps.

[3] For instance, Gigya, defined in Wikipedia (https://en.wikipedia.org/wiki/Gigya) as a "customer identity management" company, is categorized in AppFigures as a Mapping SDK.

Data going to advertisers can include a "unique identifier" to uniquely identify the individual (i.e., student or parent), tracking personally identifying information such as the user's name, email address, location and device ID use across multiple apps.

Additionally, there is one higher level of risk, called ***very high-risk.*** SDKs receive this risk attribution level if:

- AppFigures considers it an Advertising & Monetization SDK, or
- We consider it an "advertising platform". For instance, we consider Doubleclick, which AppFigures designates as a Utility, to be an advertising platform.
- The SDK appears in either the California[4] or the Vermont[5] registries of Data Brokers. Two SDKs were found in the California Data Broker registries: AdColony and InMobi.

Very high-risk SDKs routinely sync to dozens, if not hundreds or thousands, of additional partners through a complex supply side network[6] while leveraging unique mobile advertising identifiers that allow all participants in the network to create unique profiles for people, tracking people and their information across services and devices:

> *The Google Play Android Advertising ID is a unique identifier assigned to every Android device. According to Google, this identifier allows "ad networks and other apps anonymously identify a user". This unique identifier is akin to a resettable serial number assigned to a user's device, and consequently referring to the user of the device. The Advertising ID is available to all apps on the device without requiring any special permissions or consent from the user. This is often used by adtech companies to link digital profiles in order to track consumers across services and devices.*[7]

As a final assessment, the high-level functions of each SDK were examined to validate the risk attribution used in the analysis.

4 FINDINGS

Our analysis examined the following issues in order to identify potential trends and patterns:

- The information being shared,
- Magnitude of third-party data sharing as evidenced by the number of SDKs included,
- Detailed analysis of third-party data sharing behavior, including
  - External data sharing behavior trends across operating system/platform (iOS / Android),
  - External data sharing behavior trends across school types (public / private),
- The riskiness of external data sharing as evidenced by the nature of the SDKs included – in particular, examining trends related to the risk attribution for each SDK,
- Which third parties are receiving data,
- The average age of apps,
- External data sharing disclosures/labels, and

[4] Data Broker Registry | State of California - Department of Justice - Office of the Attorney General
[5] Corporations Division (vermont.gov)
[6] "Out of Control: How consumers are exploited by the online advertising industry", Consumer Council of Norway, January 14, 2020, pp. 35-39. https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[7] Ibid., p. 28.

- Schools/districts with only iOS versions of apps.

4.1 What Information Is Being Collected and Shared?

Most, if not all, of the apps seem to be uniquely identifying the user of the app through account creation, in order to send messages, upload photos, or process payments, which means the app was collecting personally identifying information (PII) such as name, age, and other information.

The Android Play Store lists all of the requested permissions by each Android app. Most (nearly all) of the examined Android apps were designed to access the following information on the device:

- Identity – known in the adtech industry as a Mobile Advertising Identifier (MAID); Android refers to this as an "Ad ID" and iOS refers to it as an "IDFA"
- Calendar
- Contacts
- Photos/Media/Files
- Location
- USB Storage

Several apps were accessing:

- Camera
- Microphone
- Device ID & Call Information

Additionally, virtually all apps also access Network Data by default. An IP address is a field of data that is hard for devices to block, and while there are permissions for expanded network access (devices on the network, access to custom ports, etc.), some version of network data should always assumed to be accessed (and potentially shared with third parties).

When the user grants permission to the requested information (listed above), it is then accessible by both the app and all the SDKs. Thus, it's information the app and SDKs *can* access, but not a guarantee that it does.

This qualitative review of the types of information collected and generated by the apps suggests that there is potential for a large amount of information that could be shared with third parties.

4.2 Magnitude of Data Sharing in Educational Apps

4.2.1 Most apps shared data, averaging over 10 SDKs per app

- Most (60.3%) of the apps (44 out of 73) had at least one SDK installed and were sharing private student data with third parties.
- The 44 apps that had SDKs included a total of 486 SDKs.
- Of the apps that included SDKs, the average number was 10.6 SDKs per app. (See Figure 2.) Note that multiple SDKs can be from a single developer, so this number is not equivalent to the number of third parties with whom data is being shared, which is lower.
- Private school apps that included SDKs had a higher average number of SDKs per app (13.8) as compared to public-school apps with SDKs (10.8). (See Figure 2.)

- Android apps included a significantly higher average number of SDKs per app (13.4) as compared to iOS apps (8.5), which is a typical pattern seen generally when comparing Android and iOS apps. (See Figure 2.)

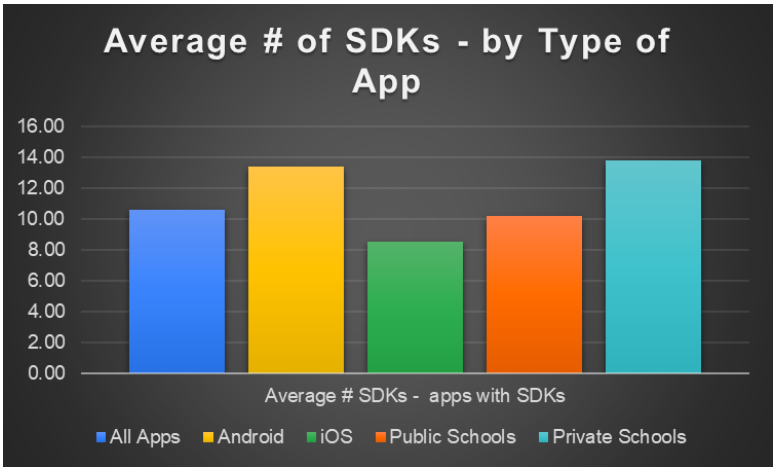


Figure 2: Average Number of SDKs per App with at least one SDK, by App Type

- Frequently – about 20% of the time – there were more than 15, and sometimes as many as 20 SDKs in a single app. The histogram in Figure 3 shows the distribution of apps by number of included SDKs.
- 29 apps didn't include any SDKs. (Figure 3.)

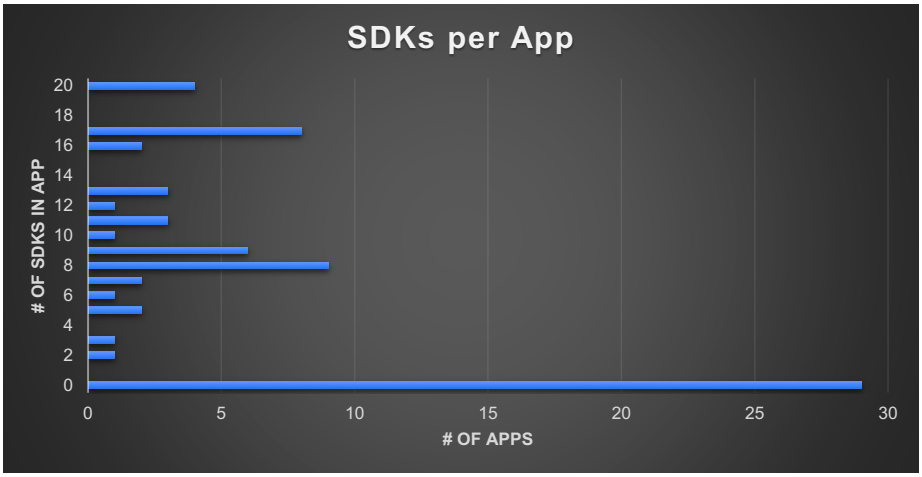


Figure 3: Number of SDKs per App Histogram

4.3 External Data Sharing Behavior

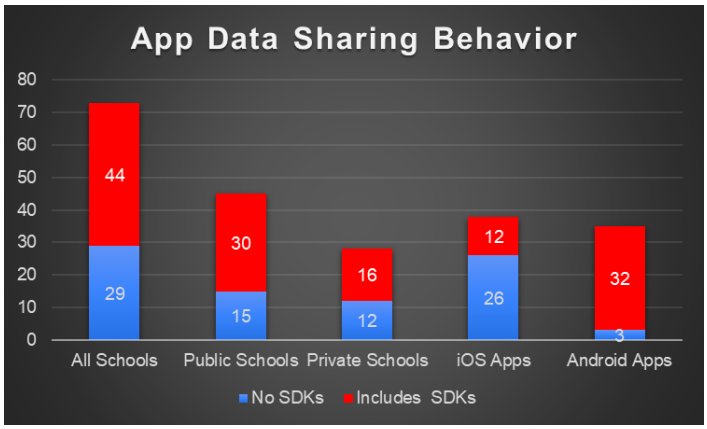


Figure 4: App Data Sharing Behavior by Type of App

Of the 44 apps that were sharing data with third parties, 73% were Android apps.

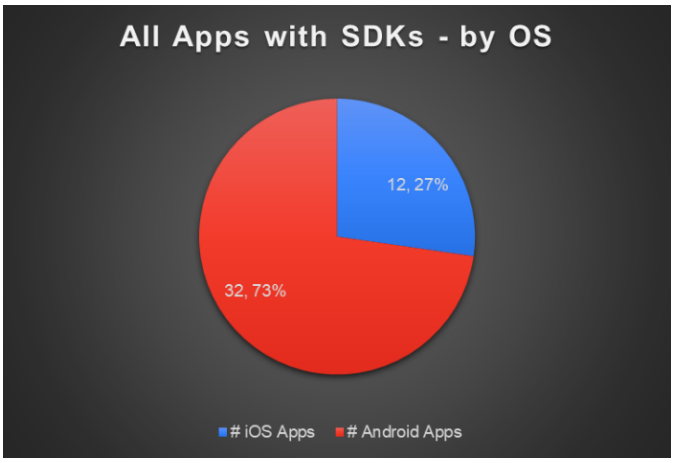


Figure 5: All Apps with SDKs by Operating System

Of the 44 apps that were sharing data with third parties, two-thirds (66%) were public-school apps.

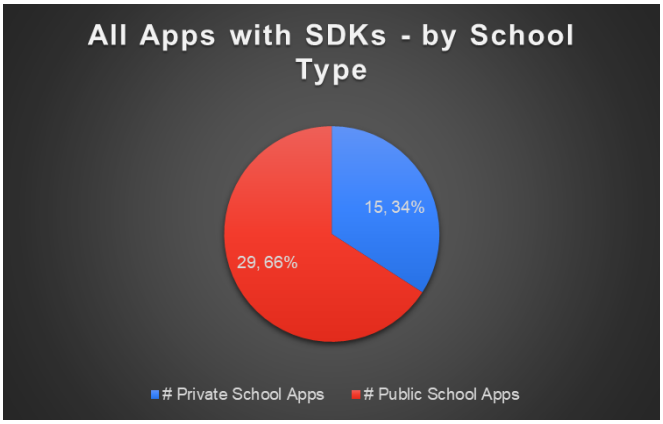


Figure 6: All Apps with SDKs by School Type

4.4 Appropriate Care of Children and Their Data

Of the schools in our study, 85% have students under the age of 13. This analysis doesn't afford a way to know how any of these third-party SDKs are tracking and handling the information of children under the age of 13. Additionally, this research did not explore the permission management practices between the app developer and the companies providing the SDKs, and if permission controls flow down from the first-party app to the third parties (prior to the app's support of Apple's ATT framework). Based on our findings, the extensive external data sharing behavior found in our analysis must be assumed to include personal data from children under the age of 13.

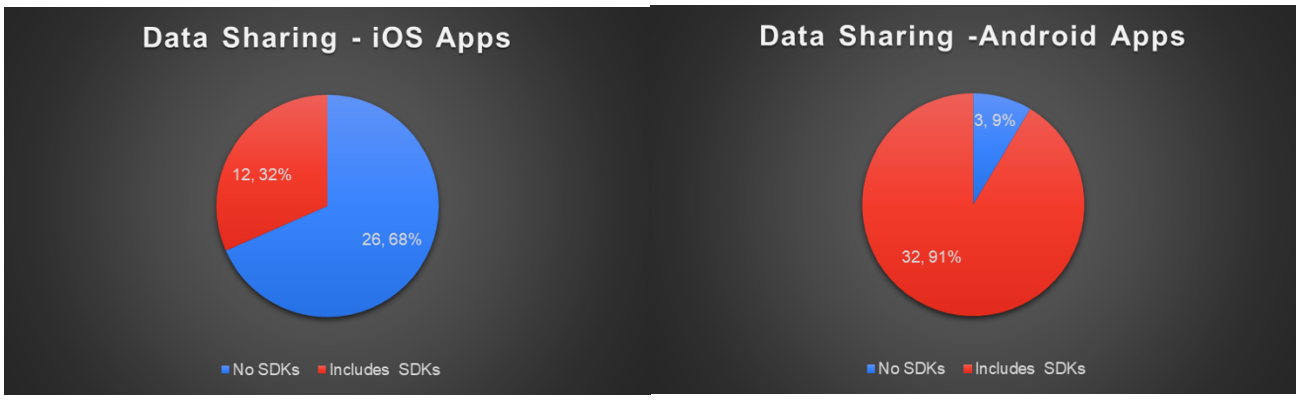
Another critical issue with school apps is that quite often, the school/district is the client to the app developer, and several of the app developer Privacy Policies assert that the student information and the control of it belongs to the institution – not the app developer. This is confusing, since [at least in the vernacular of the GDPR], the app developer seems to be the Data Controller.

Encouragingly, Google has a Family Ads Program[8] as a part of their actions to build a safer Google Play store for kids[9]. However, three SDKs designated **very high-risk** in this study (AdColony, AdMob, and InMobi) and one ***high-risk*** (Flurry) are included in the current list of self-certified "family friendly" ad SDKs, and the list hasn't been updated in a couple years. Additionally, IronSource, Vungle, Unity and Chartboost were all named SDK Developer Defendants (see Section 4.7) in the recent settlement in Northern California which should give Google sufficient incentive to overhaul its Family Ads Program.

4.5 External Data Sharing Behavior Trends Across Operating System/Platform

In addition to the previously mentioned fact that Android apps have a higher number of SDKs per app than iOS apps, there are additional observations between iOS and Android apps.

- **iOS apps are much more likely to include *no* SDKs – i.e., to be "clean" with respect to data sharing – than Android apps.**
- 68% of all iOS apps had no external data sharing, whereas 91% of all Android apps had external data sharing. (See Figure 7) This is reflecting the reality that Android, as a development platform, relies upon a number of external SDKs to facilitate app development. These findings reflect the expected pattern between iOS and Android Apps.



[8] https://support.google.com/googleplay/android-developer/answer/9283445
[9] https://android-developers.googleblog.com/2019/05/building-safer-google-play-for-kids.html

Figure 7: Data Sharing: iOS and Android

4.6 External Data Sharing Trends Across School Types

64 percent of public-school apps included SDKs, whereas only 54% of private schools included SDKs. (But as noted earlier, private-school apps that included SDKs had more of them, on average.)

Most likely, taxpayer funds were involved in financing public-school apps. Thus, taxpayers may unwittingly be supporting digital advertising businesses.

Figure 8: Data Sharing: Public vs. Private Schools

4.7 App Sharing Behavior by Risk Attribution of SDK

As noted earlier, there were 486 total instances of SDKs present in the 73 apps studied (with 44 apps including one or more SDK). Figure 9 shows the distribution of those 486 SDKs by risk attribution. ***The majority (58%) of SDKs included in apps studied were designated as high-risk.***

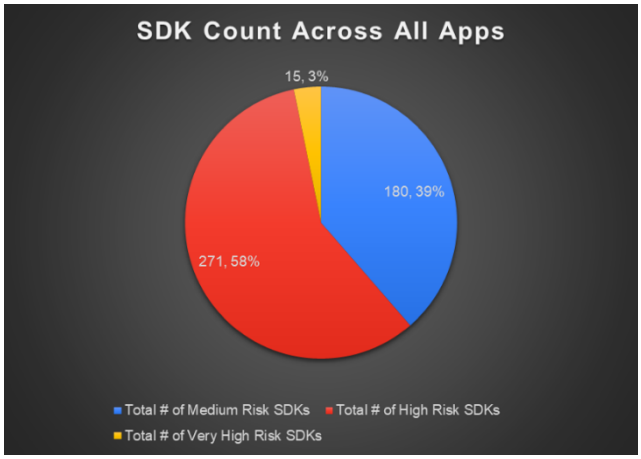


Figure 9: SDKs by Risk Attribution

- Nearly 20% of apps that included SDKs included ***very high-risk*** mobile advertising platforms. (See Figure 10)

- 95.5% of apps that included SDKs included high-risk SDKs, sharing data with high-risk third parties – advertising and advertising related platforms, including Google, Facebook, Yahoo, and Twitter.

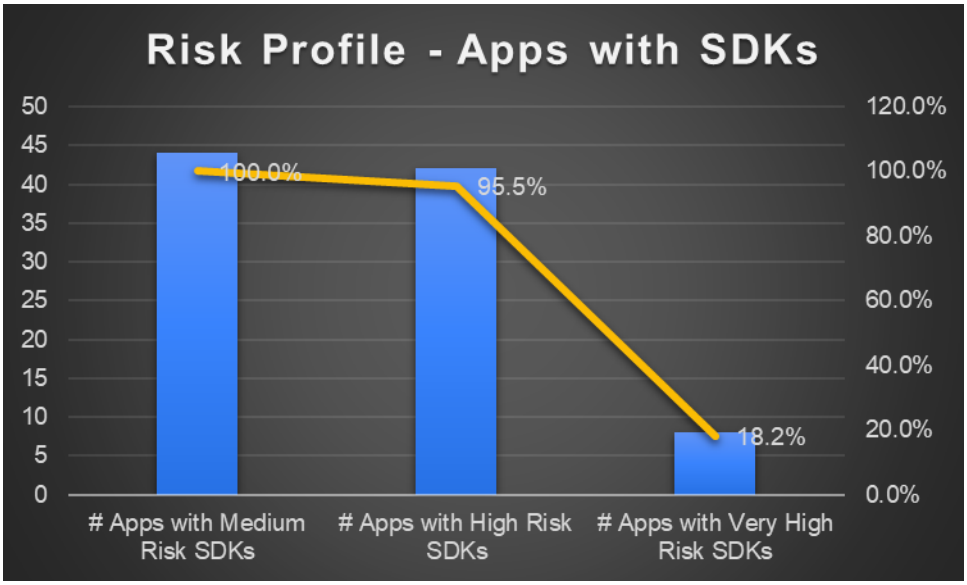


Figure 10: Risk Attribution Analysis Across Apps with SDKs

Figure 11, below, shows the percent of Android/Apple apps that contain medium/high/very high-risk SDKs, as a percent of the total number of Android or Apple apps that include SDKs.

- ***Android apps are about 8 times more likely than iOS apps to include very high-risk SDKs.***
- ***Android apps are 3.5 times more likely than iOS apps to include high-risk SDKs.***

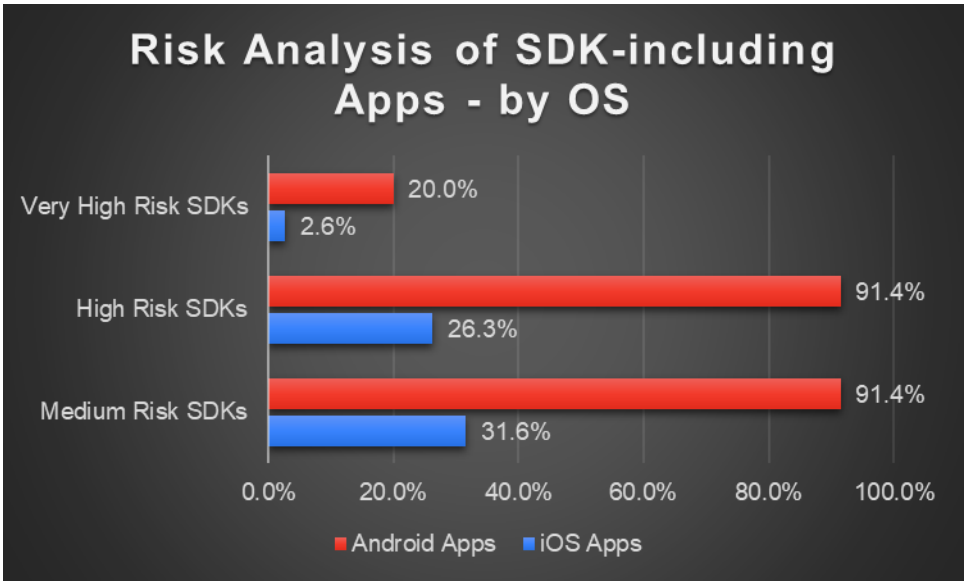


Figure 11: Risk Analysis of SDK-including Apps by Operating System

Similarly, Figure 12, below, shows the percent of public/private-school apps that contain ***medium/high/very high-risk*** SDKs, as a percent of the total number of public/private-school apps that include SDKs.

- ***Very high-risk*** SDKs were *only* found in public-school apps; and nearly 20% of public-school apps that had SDKs included *very high-risk* SDKs.
- While *very high-risk* SDKs were found only in public-school apps, public and private-school apps are comparable in the likelihood of including *high-risk* SDKs.

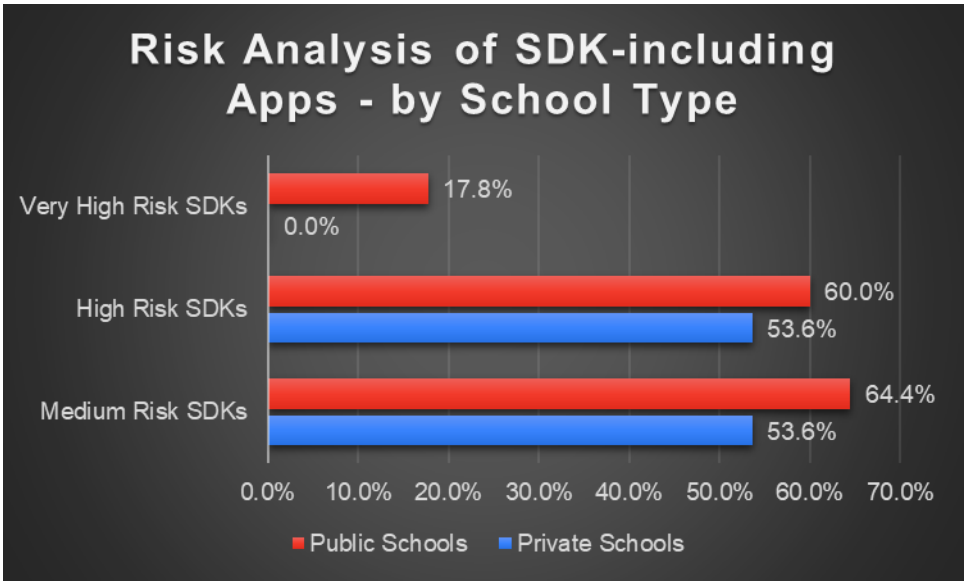


Figure 12: Risk Analysis of SDK-including Apps by School Type

4.8 What Third Parties are Receiving Student Data?

The apps in our study used 56 unique SDKs.

Of those SDKs, the owners of the most SDKs were Google (12), Facebook (7), Apple (7), Amazon (3), Square (3), Twitter (2) and Adobe (2).

SDKs owned by Google and Facebook were included 306 times in our studied apps. Said another way, ***63% of all SDKs used by the studied educational apps were owned by either Google (48.6%) or Facebook (14.4%).*** Additionally:

- ***100% of the Android apps that included SDKs sent data to Google.***
- 9 (12%) of the apps shared data to Google's AdMob SDK, sending personal information to Google's mobile advertising products.
- At least 17 (23%) of apps with Google SDKs had six or more Google SDKs installed, including Google Maps, Google Sign-In, AdMob, Tag Manager and other Google Products.
    - One of Google's SDK products in the school apps is Fabric, which was previously owned by Twitter.
- 19 (22%) of the apps shared data to Facebook, with data going to 4 or more Facebook SDKs including Facebook Analytics, Facebook Share, Facebook Login and Facebook Bolts SDKs.
- 5 (7%) of the apps shared data to Twitter SDKs, with most of them being for Twitter's Login SDK, and at least one app (South Dakota, iOS app) sharing data to Mopub, Twitter's mobile advertising subsidiary (and *very high-risk* attribution).
- 6 (8%) of the apps shared data to Yahoo's Flurry Analytics SDK which is an SDK that has advertising ingestion functionality (*high-risk* attribution).

The top 10 most frequently included SDKs are shown below in Table 1.

SDK Name	Occurrences	Owner	Risk Designation
Firebase	34	Google	Medium
Google Sign-in	33	Google	High
Firebase Messagig	31	Google	High
Firebase Analytics	30	Google	High
OK HTTP	30	Square	Medium
Okio	29	Square	Medium
Google Maps	28	Google	High
Fabric	21	Twitter	High
Crashlytics	21	Google	High
Bolts	21	Facebook	Medium

Table 1: Top 10 Most Included SDKs Across All Apps

As can be seen from Table 1, six of the top 10 most included SDKs are owned by Google. And six of the 10 most included SDKs are deemed ***high-risk*** SDKs.

As stated earlier, the most troubling aspect of this kind of data sharing is that there is no way to know how these large platforms are handling the data of school-age children, especially those under the age of 13. Are these companies tracking the age of the information of the data subject for whom they are collecting information?

In a recent groundbreaking legal win[10] for consumers – and children, in particular – several large developers of apps for children were mandated by the U.S. District Court for the Northern District of California to remove or disable tracking – which is typically accomplished through SDKs. One of the authors of this paper tracked the publicly available settlement information[11] which holds both the developers of the apps and the companies behind the included SDKs responsible and accountable. The settlement agreements include actions such as:

- Removing or disabling SDKs in *all* of their childrens' apps within a limited time frame (four months for Disney),
- Delete all ingested childrens' data (Twitter), and
- Being banned from ingesting device IDs for three years (Comcast).

In the settlement information, four SDK developers from our school app research were named as "SDK Developer Defendants": Twitter, AdColony, Flurry, and InMobi, which means that all four of these developers have specific obligations relating to the data of children under 13 years of age.

4.9 App Labeling Deficiencies

4.9.1 Inadequate Information About Which Third-Party SDKs Are Included

Google doesn't have a privacy label similar to Apple, so Android users have no privacy information at all supplied at the Google Play Store level. However, Android apps do list all the permissions for an app before you download the app.

[10] "Disney and Ad-Tech Firms Agree to Privacy Changes for Children's Apps", Natasha Singer, *New York Times,* April 13, 2021, https://www.nytimes.com/2021/04/13/technology/advertising-children-privacy.html
[11] https://twitter.com/thezedwards/status/1382182587628544000

Neither Apple nor Android discloses the names of the SDKs and SDK owners to users, either in the app or in the app stores. So even though Google, Facebook, Twitter and several other well-known companies are the primary recipients of student data coming from apps, the ***people using the apps have no real way to know which platforms will receive their data.*** Once again returning to Me2B vernacular, users are in undisclosed Me2P relationships with the SDK owners.

4.9.2 App Stores Privacy Policy Links

Both the Apple and Google Play app stores include links to Privacy Policies. Two types of problems with the privacy policy Links were observed:

- Missing or broken links, and
- Policies that focused on the developer's website practices, not policies that applied to the mobile app.

In both of these cases, the end result is that there is literally no privacy policy or data use information relating to the app prior to downloading the app, especially if there is also a missing Apple Privacy Label, or for Android apps, for which there is no privacy label.

4.9.3 App Age Rating Older Than Youngest Students

For four apps, the app's age rating in the app store indicated an older age than the youngest students in the school.

4.10 Privacy Policy Deficiencies

4.10.1 Privacy Policies Apply to the Developer's Website

Ten of the apps' Privacy Policies appeared to cover only the app developer's website, not the mobile app. It's not unusual for websites and apps to have distinct privacy policies, particularly in the case of websites and apps that are developed, hosted, or operated by different entities, since different developers/operators may have different internal privacy practices and technology even if they were working on behalf of the same school. Thus, it would be reasonable to expect that the app's privacy policy and data use information prior to download and installation is unclear or unknown.

4.10.2 Privacy Policies Apply to the Educational Institution

Many of the Privacy Policies make clear that the policy covers the relationship with the Client, meaning the educational institution, and that the end users' – students' and parents' – information is covered by the institution and the institution's privacy policy. The institution's privacy policies, however, are not linked in the app stores.

Here's an example from Privacy Policy for an app developed by Apptegy, Inc. [https://www.apptegy.com/privacy-policy/]:

> *"Simply put: when we process personal information about you that is provided by your educational institution or organization (or by you or another individual under your educational institution's or organization's account), we are not responsible for the disclosures made by your educational institution or organization (or those individuals under the institution or*

organization account). It is your educational institution or organization that has the responsibility to protect your privacy."

4.10.3 Privacy Policy Exclusions for Children Under the Age of 13

Several Privacy Policies explicitly exclude children under the age of 13 even though the apps are for schools that include students under the age of 13. Here's an example from the Apptegy privacy policy excerpted above, which is connected with a K-12 school district that is labeled by the app store as "E for Everyone:"

> *"We do not permit individual users or individual accounts for individuals under the age of 13. In addition, we do not knowingly collect any information about or from children under the age of 13, except when an educational institution or organization (or an individual under an institution or organization account) provides information about or from a student under the age of 13 via our goods and services."*

It should be apparent to the developers of an app for a K-12 school district that some students would, by their very nature, be individuals under the age of 13. The statement that users under 13 are not permitted on the app either lacks nuance that needs to be revised for clarity or is simply a "legal fiction" included in the policy by the developer as an attempt to stay out of the purview of COPPA (a difficult-to-comply-with law that significantly regulates data collection from users under 13).

4.11 Average Age of Studied Apps

4.11.1 Most Apps Were Not Current with the Latest Privacy Protections

As noted above, disclosures were lacking on mobile apps and app stores. The inadequate disclosures are exacerbated by slow updates, which means even when new standards are deployed, educational apps may be late to adopt them. For instance, the recent Apple privacy label is only required for apps which have been updated since December 2020.

The majority (74%) of Apple apps reviewed (28 out of 38 apps) had not been updated since December 2020, and so were not subject to Apple's recent requirement to provide the Apple privacy label. A small but significant percentage of the apps, almost 7% (5 out of 73), hadn't been updated in as much as four years, since 2017.

Due to slow updates, these apps may lag – possibly up to a year behind – to incorporate emerging major privacy protections such as the newly required Apple AppTrackingTransparency framework, which requires the app to obtain permission for any data sharing with tracking third parties, such as advertising networks. It's likely that, at publication time, 100% of all iOS apps in this study will not be compliant, and users of these school apps still won't be able to opt out of third-party tracking.

- The average age of the educational apps was 11.5 months. (See Figure 13.) ***Educational apps are being updated on average about once a year.***
- Private-school apps were about four months more current than public-school apps.
- The oldest apps on average were Apple apps for public schools. Since Apple apps are likelier not to include SDKs, this is one privacy concern these apps may not have, but they may still be missing newer privacy updates.

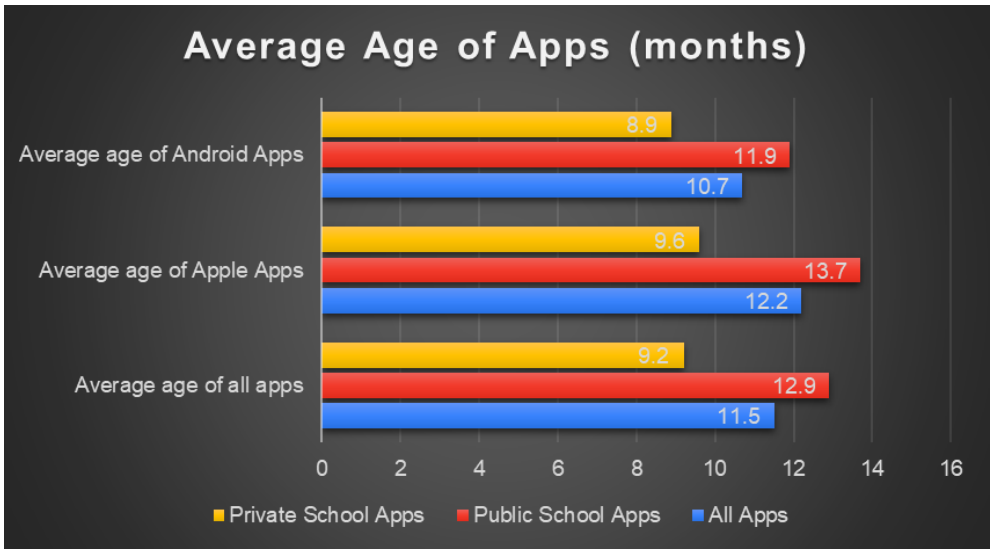


Figure 13: Average Age of Educational Apps

4.12 Developer Analysis

Of the school apps studied, 99% were developed by professional app development companies. There was one instance where the app appeared to be "home grown". Notably, this app had the highest number of ***very high-risk*** SDKs included. (The Alliance reached out to the school in question to alert them of this finding. At publication time, no response was received yet.)

Of all school apps studied, 77% were developed by six specialized "ed tech" companies: LegitApps, Apptegy, Blackboard, SchoolInfoApp, Straxis and Web4u Corp.

Virtually identical to our overall, SDKs appeared in 61% of the apps built by these top six developers.

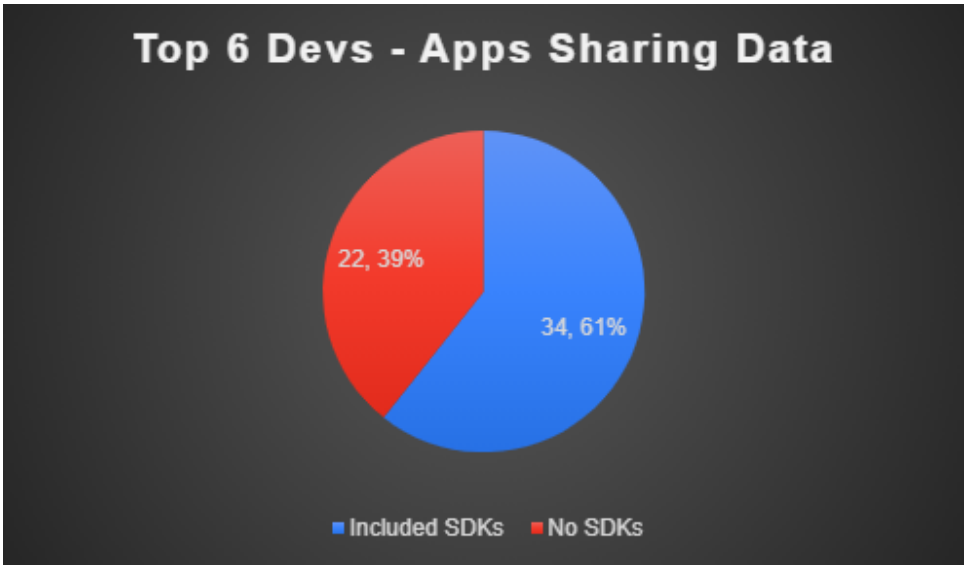


Figure 14: Top Six Developers Apps Sharing Data

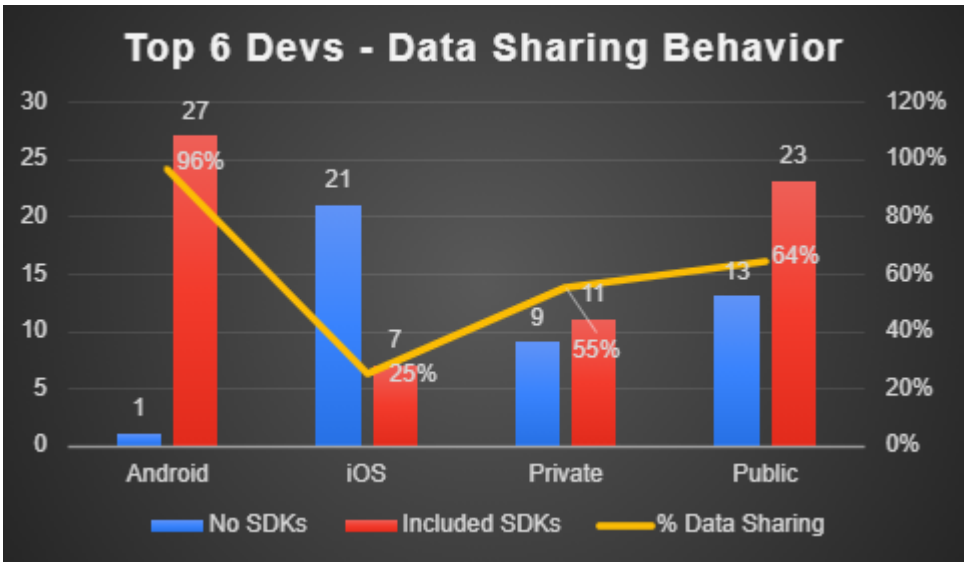


Figure 15: Data Sharing behavior in Apps Built by Top 6 Developers

Somewhat higher than the behavior across all apps, 79% of the top six developers' apps sharing data were Android apps (compared to 73% across all apps).

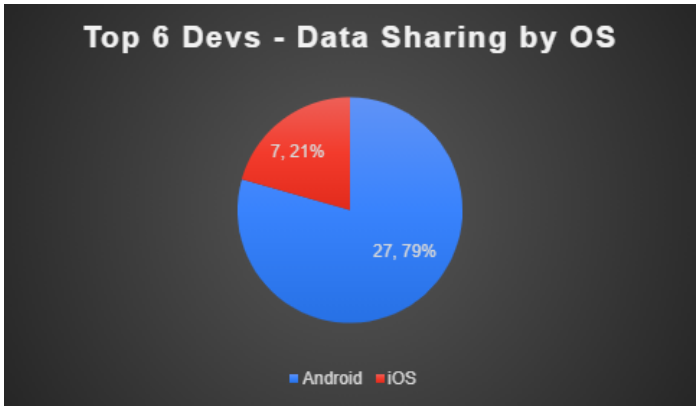


Figure 16: Data Sharing in Apps Built by Top 6 Developers by Operating System

In the 34 apps developed by the top six developers that included SDKs, 68% of them were for public schools. This compares to the total sample, which had 66% of the apps with SDKs being for public schools.

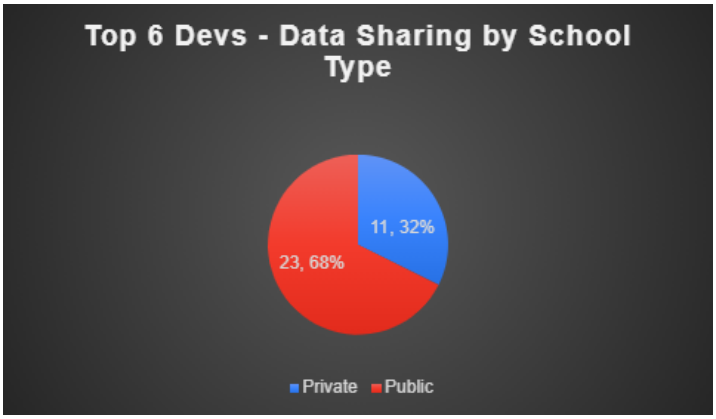


Figure 17: Data Sharing in Apps Built by Top 6 Developers by School Type

The top developers were closely examined because ***schools rely on these companies for their expertise in understanding the complex privacy issues involved with working with personal student data***. With the majority of these apps sharing student information with third parties, there are several outstanding questions:

- Are the developers aware of the risks of the SDKs in their apps?
- Are the developers alerting their clients as to the potential risks?
- Are the developers responsible for submitting deletion requests on behalf of the students to the SDKs that ingested their data?

4.13 Missing Android Apps

Three of the schools/districts with Apple apps had no corresponding Android app.

While this is a small percentage of our findings at 7.9% of the schools, this finding could be indicative of a larger problem where students who only have Android devices will be left behind. Since Apple devices are historically more expensive than Android devices[12], this could be another facet of the digital divide.

5 RECOMMENDATIONS

The Me2B Alliance offers the following recommendations to make school apps safer for students and their families.

1. School apps for primary and secondary schools must *not* share data with third parties, and thus must *not* include *high-risk* or *very high-risk* SDKs.

2. App developers creating apps for use by schools and school districts must be transparent, up to date, principled, and rigorous about their privacy protection practices and processes. Schools can't be expected to be technical and privacy experts.

3. Apple's App Privacy Labeling is a step in the right direction. We urge Google to offer the same protections in their Play store – especially as they have recently added Privacy Labels to the Chrome Extension store.

4. The Apple and Google app stores must update (or create, in the case of Google) privacy labels to include a list of all the SDKs that are installed in every app, including the name of the SDK owner/parent company. That way parents and students can make informed decisions about where they want to send their data.

5. Google must revisit its Family Ads Program to ensure adequate protections and practices are in place. Additionally, it must perform independent validation of the self-provided assessments.

6. Apps used by children must improve their Privacy Policies.

[12] "Here's Why Developers Keep Favoring Apple Over Android", Jim Edwards, *Slate*, April 4, 2014, https://slate.com/business/2014/04/apple-vs-android-developers-see-a-socioeconomic-divide.html.

7. Privacy Policies for institutional clients must make clear who has access to students' data (the app developer, the institution, or both), and who is responsible for ensuring that data is appropriately protected, particularly for students under the age of 13.

6 FOR FUTURE STUDY

This research is just a starting point for additional investigation – either by the Me2B Alliance or by other interested organizations. Several questions warrant deeper exploration:

- Should taxpayer money ever be used to build apps that send data to *high-risk* advertising and analytics companies such as Google, Facebook, Twitter, Yahoo, etc.? Some examples may be government or civic apps.
- What is the process by which public schools requisition educational apps and is there anything that can be learned from it?
- What sorts of auditing and governance can be applied to companies that ingest student data, especially for students under the age of 13 who are protected by COPPA?
- Does it make sense to mandate any practices, such as mandatory data deletion for data subjects under the age of 13? How can public and elected officials be assured that advertising SDKs are upholding the requirements?
- Should schools be required to update apps for students at some regular interval? Is once a year sufficient?
- How can schools efficiently keep apps updated with emerging privacy enhancements, whether industry norms (like Apple's privacy label), or local or federal regulations?
- Should there be an "access" requirement (potentially under the 1964 Civil Rights Act) that requires schools or school districts to make sure that versions of their apps are available to all users on all platforms, to ensure equity of access to educational tools?
- Why are developers routinely including questionable APIs in Android apps, but not in Apple apps?

7 CONCLUSIONS

Our analysis was not intended to be comprehensive. In our review, we chose schools and school districts, and the educational apps they use, at random. Nevertheless, the frequency with which apps were using SDKs and sharing personal data of students with *high-risk* advertising and analytics companies is disturbing. Table 2 below is a summary of the likelihood of an educational app will share personal data with third parties based on our sample set.

	All	iOS	Android	Public Schools	Private Schools
Likelihood of 3rd party data sharing (SDKs)	60%	32%	91%	64%	54%
Average number of SDKs	10.6	8.5	13.4	10.2	13.8
Likelihood of Very High Risk SDKs	11%	3%	20%	18%	0%
Likelihood of High Risk SDKs	58%	26%	91%	33%	96%
Likelihood of Medium Risk SDKs	60%	32%	91%	64%	54%

Table 2: Summary Findings

The main conclusions of this research are:

1. The majority of apps (58%) were sending student data to *high-risk* adverting and analytics third parties.

2. iOS apps are safer/less risky, on the whole.

3. Android apps are much more likely to send data to third parties.
    a. 100% of the Android apps that included SDKs were sending student data to Google.
    b. 67% of Apple apps that included SDKs were sending student data to Google.
    c. 49% of total apps were sending student data to Google.

4. Public-school apps are more frequently sending data to third parties, as compared to private schools, but both are sharing student data in more than 50% of the apps.

5. Taxpayers may be paying for educational apps to collect and share student data with some of the leading advertising and analytics companies in the world.

6. App labels and other information in the app stores don't provide adequate or accurate information.

7. School apps aren't being updated in a timely manner relative to the introduction of privacy enhancing practices (like the Apple Privacy Label, Apple's imminent AppTrackingTransparency Framework, and other practices).

8. SDKs don't discriminate data sharing practices based on the age of the data subject; they just send data. Student data from children under the age of 13 is being sent to high-risk advertising and analytics companies with no distinguishing tags, and likely is not being handled with the precautions required.

The Me2B Alliance, as a nonprofit fostering the respectful treatment of people by technology, is a new type of standards development organization that is working to define the standard for respectful technology. Scenarios like the ones described in this report – where user data is being abused, even inadvertently – highlight the types of issues we are driven to prevent through independent testing, as well as education, research, policy work, and advocacy.

We welcome your thoughts and feedback. If you are interested in learning more about our independent testing and audits, contact us at services@me2ba.org.

If you are interested in supporting the Me2B Alliance to perform more research like this, contact us at admin@me2ba.org.

The data used in this report is available upon request by contacting us at admin@me2ba.org.