Privacy Considerations as Schools and Parents Expand Utilization of Ed Tech Apps During the COVID-19 Pandemic

September 1, 2020

By Quentin Palfrey, Nathan Good, Lena Ghamrawi, Will Monge, and Willie Boag

As educators and parents struggle to adapt to social distancing requirements amid the continuing COVID-19 pandemic, ed tech apps have become an increasingly popular tool to assist with remote teaching and learning. To assist in ensuring the trustworthiness of the ed tech app ecosystem, the International Digital Accountability Council (IDAC) investigated the privacy practices of 496 global ed tech apps spanning 22 countries.

Overall, our investigation demonstrated that ed tech companies and developers generally incorporated privacy protection into the design of the apps. Our investigation did not reveal obviously intentional or egregious misconduct.

Nevertheless, our investigation uncovered some privacy and security risks that merit remediation. This report seeks to highlight some areas where there is a need for improvement to conform with privacy and security best practices. Additionally, in the spirit of seeking to help distance learning succeed, we make some general suggestions for consideration in improving the trustworthiness of the ed tech app ecosystem.

IDAC's investigation revealed that some apps: (1) share location data and persistent identifiers with third-parties; (2) expose personal data in their URLs, raising security concerns; (3) allow a large number of third-parties to collect user information; (4) engage in ID-bridging, a practice that allows apps to circumvent users' privacy controls; and (5) embed potentially invasive and unnecessary software development kits (SDKs).

Our investigation concludes that, while most ed tech apps we tested act in ways that align with users' privacy expectations, there are gaps that developers and platforms should review and remedy in order to promote user trust and encourage widespread adoption.

Launched in April 2020, IDAC is led by an experienced team of lawyers, technologists, and privacy experts with a shared goal of improving digital accountability through investigation, education, and collaboration. As a nonprofit watchdog, IDAC investigates misconduct in the digital ecosystem and works with developers and platforms to remediate privacy risks and restore consumer trust.[1]

Methodology

Our goal was to identify a wide range of apps that teachers or parents might find in seeking tools to assist with remote learning, rather than focusing exclusively on apps that are widely used by school districts with established procurement protocols.

IDAC's investigation consisted of both manual and automated testing of a universe of apps that encompassed ed-tech/virtual classroom apps, educational content apps ("learning apps"), language learning apps, learning games, library or book reader apps, study help, and team communication tools that are deployed in the context of remote learning.

We identified these apps based on teacher surveys we administered, as well as the top educational apps on the Google Play Store.[1] As described further below, we conducted manual testing on a universe of 98 unique apps that were available as of July 15, 2020 across 22 countries[2] on two platforms (iOS and Android).[3] Additionally, we ran automated tests on 421 Android apps.

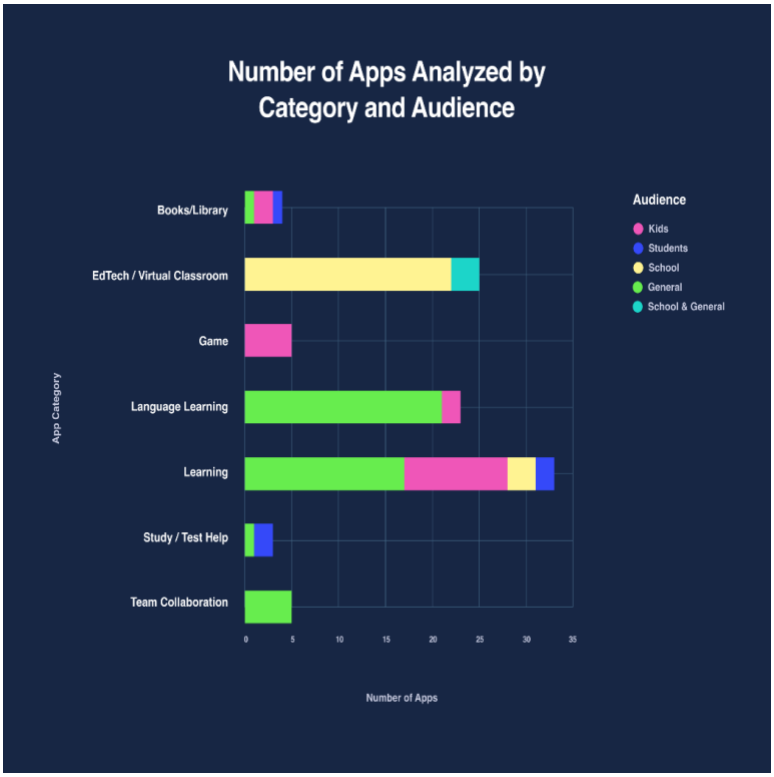

Figure 1: *A breakdown by the potential audience for these apps across each of the above categories.*

Manual Testing

With respect to our manual testing, we conducted static and dynamic manual analysis tests on 78 Android and 45 iOS apps to determine how they operate in real time. Using Android and iOS devices, we downloaded the apps and interacted with them in the way a typical user would, trying to use as much of the app as possible to test all potential subsections and screens. Next, we ran our analysis on the network traffic and additional operating system information that was generated while we were interacting with the apps. From these results, we were able to observe a variety of behaviors associated with the collection and transmission of personal information, including the types of personal data these apps collect, to whom the data is being sent, the types of software development kits (SDKs) present in the apps, and other data transmissions.[4]

[1] We used the "Education" and "Educational Game" categories.
[2] The 22 countries only encompass the manual tests we ran.
[3] We manually tested a total of 123 apps (78 Android apps and 45 iOS apps) but there was some overlap so the total number of unique apps tested is 98.
[4] Although our team was able to analyze these apps, we were not able to thoroughly test a few apps due to the strict verification controls these apps have in place. For example, some apps required a school-provided identification number, while others required a unique teacher-issued number to login and create an account.

Automated Testing

In addition to the manual testing we conducted on 98 unique apps, we also conducted automated testing on 421 Android ed tech apps. The automated testing consisted of static and automated dynamic tests. Here, we performed “app fuzzing” or “monkey testing”, in which a script interacts with an app by sending a series of stochastic actions (i.e., taps and swipes). The automated test is performed on each app for approximately five minutes.[5]

The full list of apps that we tested can be found in Appendix A.

Demographics

The manual apps we investigated span across 22 countries, with the majority of apps (53) being developed in the United States. The chart below highlights the distribution of countries that were included in this report.

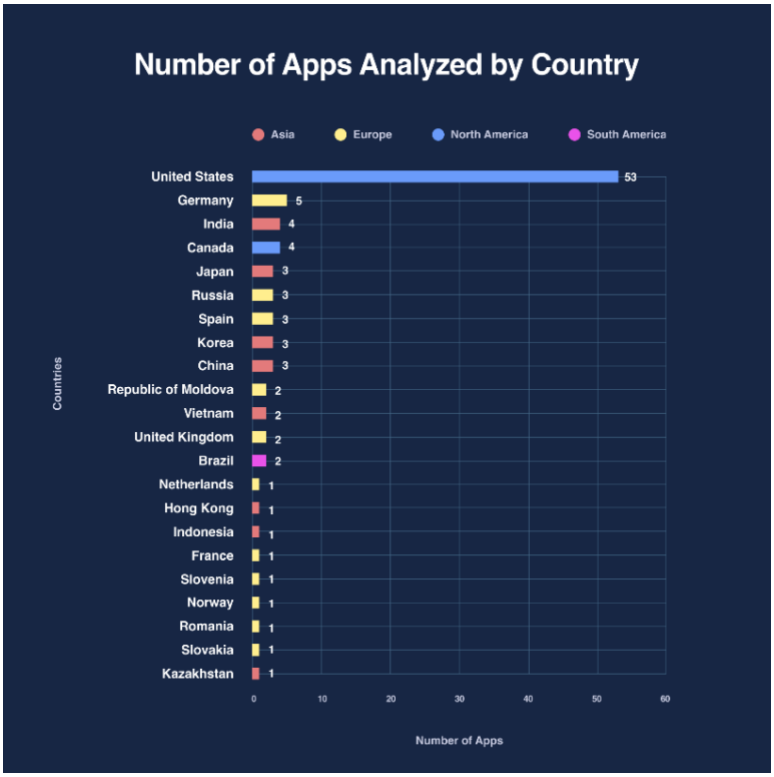

Figure 2: *The distribution by country of each app developer among the 98 manually-tested apps.*

[5] These automated tests are not as thorough and complete as our manual tests, but the patterns that arise from these tests help illustrate some privacy practices of ed tech apps at a larger scale.

Table of Contents

I. Key Findings

The investigation revealed areas for improvement for app developers and companies. However, we did not identify conduct that we would characterize as egregious or evidently willful. Our five key findings are outlined below.

A. Location and Persistent Identifiers - Data Collection and Sharing

The first area of concern relates to the collection and sharing of location data and persistent identifiers. Persistent identifiers are tied to the hardware of the device and cannot be reset, making it easy for third-parties that have this information to track users and make inferences based on their device activity.

Location tracking -- whether through collecting location or persistent identifiers -- is particularly problematic when the data subjects are children. Collecting this information and sharing with third-parties allows for the possibility that this information will be manipulated, misused, or monetized.

Our tests identified instances where location data and persistent identifiers were transmitted from the device to a third-party, raising concerns about potential long-term tracking.[6]

Manual Tests

In the course of our investigation, we observed one app, *Shaw Academy*, collecting location data and sending it to third-parties. Our investigation revealed additional concerns with Shaw Academy's privacy practices, including:

- **Location Sharing.** The app shares location with WebEngage, a marketing third-party service that allows for behavioral segmentation and advertises[7] the ability to send targeted advertisements. Shaw Academy's privacy policy states that they collect location data "[t]o provide location-based services," but the privacy policy does not elaborate on what those services are.[8] While Webengage's services may be useful for Shaw Academy, it is unclear why collecting and sharing user location is necessary for the app to provide its services.

- **ID Bridging.** The app shares both the users' Android ID and Android Advertising ID (AAID) with Webengage. As discussed further below in section D, this practice is known as ID-bridging. Android developer policies prohibit ID bridging because it allows apps to circumvent privacy controls.

- **Aggressive Notifications.** The app partners with Webengage, a third-party service, to collect payment information. Shaw Academy -- via Webengage -- places considerable pressure on users to provide their credit card information. Shaw Academy sent 12 email reminders within nine days to our team. They also sent texts and phone call reminders. Examples of Shaw Academy's email subject lines include, "Urgent action required" followed by "Warning: urgent action required."

[6] This practice was only observed in the Android apps we tested.

[7] https://www.youtube.com/watch?v=TawD7ObcX3w

[8] https://www.shawacademy.com/privacy/

Automated Tests

Our automated tests of the larger pool of 421 Android apps revealed that 19 apps were collecting and sharing location data. Seven apps were collecting persistent identifiers. Some of these apps may use location data for legitimate purposes. For example, the *Star Tracker* app may use geolocation data to show users where constellations are in relation to their location.

However, it is not immediately obvious why other apps, such as *HelloTalk* and *Learn Python*, request user location information. *HelloTalk's* privacy policy does not mention the collection of location data.[9]

Learn Python's privacy policy discloses that they collect location data but it does not make it clear why location data is needed for them to facilitate their app, other than the fact that the app offers a "Discover Peers" feature to find nearby users to form a community and to display location information in users' profiles (e.g., Juan is a level 7 programmer from Spain with 16,000 followers).[10]

Further, our automated tests demonstrated that of the seven apps collecting persistent identifiers, three of which collect location data as well. The apps that collected both location and persistent identifiers were *Star Tracker*, *Hello Talk*, and *Ready4GMAT*.

Persistent identifiers such as Wi-Fi MAC, Router MAC and Router SSID are known surrogates for location data. Persistent identifiers are tied to the hardware of the device, making it possible for entities that obtain this data to infer and track a user's location.

By collecting these persistent identifiers, apps can circumvent location privacy controls and bypass standard mechanisms for collecting location. These persistent identifiers effectively allow the app to infer users' location, as well as to enable the app to track users over long periods of time.[11] Users cannot reset these identifiers. The only clear way to avoid this type of tracking is to obtain a new device. In our view, it is difficult to justify the purpose for the collection of these identifiers in the context of ed tech apps where many users are children.

The table below identifies the seven apps we observed collecting persistent identifiers and/or location.

App Name	Data Collected
ENEM 2020 Me Salva!	-IMEI
HelloTalk	-IMEI -WiFi MAC -Geolocation
Qanda: Free Math Solutions	-IMEI -Router MAC

9 https://www.hellotalk.com/privacy_policy.html
10 https://www.sololearn.com/privacy-policy
11 https://digitalwatchdog.org/trend-report-android-apps-inferring-location

Ready4GMAT	-SIM ID -HWID -IMEI & IMSI -Router MAC -Router SSID -Wi-Fi MAC -Geolocation
SAT Vocabulary	-HWID
Star Tracker	-Router MAC -Router SSID -Geolocation
Диктант (Dictation)	-Router MAC -Router SSID

The following 16 apps were observed sending location data:

- BYJU'S – The Learning App
- ISS Detector
- ISS Live Now
- Learn C#
- Learn C++
- Learn HTML
- Learn Java
- Learn JavaScript
- Learn Python
- Learn SQL
- Meritnation: CBSE, ICSE & more
- Paripath
- PlantNet Plant Identification
- Quiz Patente Ufficiale 2020
- Spacecraft Models 3D and Space Exploration
- Star Walk 2 Free

For more information refer to Appendix B.

B. Personal Data Exposure in URL Query Strings

Our investigation revealed some security vulnerabilities that should be resolved. Most concerning was that some apps sent personal data including name, email, and city, through the query parameters of the URL.

In four of the Android ed tech apps we manually tested, we identified a security vulnerability: data exposure in URL query strings. We observed these apps sending personal data including name, email, and city through the query parameters of the URL.

Personal data should not be left unprotected, especially when being transmitted over the internet. As suggested by the Open Web Application Security Project, this is a risky practice because it exposes personal data in URLs, allowing attackers to view and access this data, even when the transmission is performed over a secure HTTPS connection.[12] Google's Policies specifically advise developers against embedding personal data in URLs as part of their *Best Practices to Avoid sending Personally Identifiable Information*.[13] As an alternative, "[i]n most of these cases, the PII in the URL can be replaced with a unique site-specific identifier."

Less concerning -- but still problematic -- were the 13 apps we found that embedded the AAID into URLs. The practice of exposing the AAID in this fashion is not expressly prohibited by Google.[14] However, exposing the AAID does not align with best practices. Instead, we recommend including that information in the payload or generating a universally unique identifier (UUID) as an alternative identifier.[15]

The following apps were observed sending information through URL query strings.

App Name	Data Exposed in URL Query
HelloEnglish: Learn English	Email Address, Name, AAID
Learn Languages with Memrise	Email, AAID
NCERT Books	City Name, AAID
Periodic Table 2020- Chemistry	City Name, AAID
Duolingo	AAID
Byju's Learning App	AAID
Babbel	AAID
Busuu	AAID
Quizlet	AAID
Cake	AAID

12 https://owasp.org/www-community/vulnerabilities/Information_exposure_through_query_strings_in_url
13 https://support.google.com/adsense/answer/6156630?hl=en
14 https://support.google.com/admanager/answer/7686480?hl=en
15 https://segment.com/blog/a-brief-history-of-the-uuid/

Lingualeo	AAID
Vedantu	AAID
Learn English Phrases, English Translator	AAID
TO-FU oh!SUSHI	AAID
Mondly	AAID
4Pics 1 Word	AAID
Kobo Books	AAID

For more information refer to Appendix C.

C. Third-Party Communications

Our investigation also revealed concerns about the transmission of data to third parties. Using specially instrumented hardware on the mobile devices, we were able to inspect the transmissions from the device to third-parties. Those communications included personal data elements such as:

- Personal information (e.g., name, email);
- Device information (e.g., IMEI, operating system, carrier, AAID, Android ID);
- Contextual information (e.g., WiFi, router, MAC, location); and
- App information (e.g., username, password, specific information shared with apps such as age).

Figure 3: *The apps that communicated with the most third-parties for iOS apps.*

Manual Tests

79 of the 123 apps we manually tested were observed communicating user data with third-parties, which we define as any entity that is not the developer of the app or a parent company of it. On average, each ed tech app communicated with three third-parties. Our tests do not provide insight into what these third-parties do with the information they collect from ed techs apps, but we remain aware of the fact that user data is being shared externally, sometimes without the users' knowledge.

We identified over 140 third-party companies receiving user data from the ed tech apps we tested. We analyzed the frequency of these third-parties across the ed tech apps we tested. We found that 40 third-parties receive data from multiple apps within our testing list. For example, Facebook receives data from 39 apps, Google-

owned AppMeasurement from 15 apps, Branch.io from 14 apps, Google from nine apps, and Flurry from nine apps.

Our investigation did not reveal any misconduct by these third parties, but the scale and opacity of the data-collection is noteworthy and presents some risks to the health of the ed tech ecosystem.

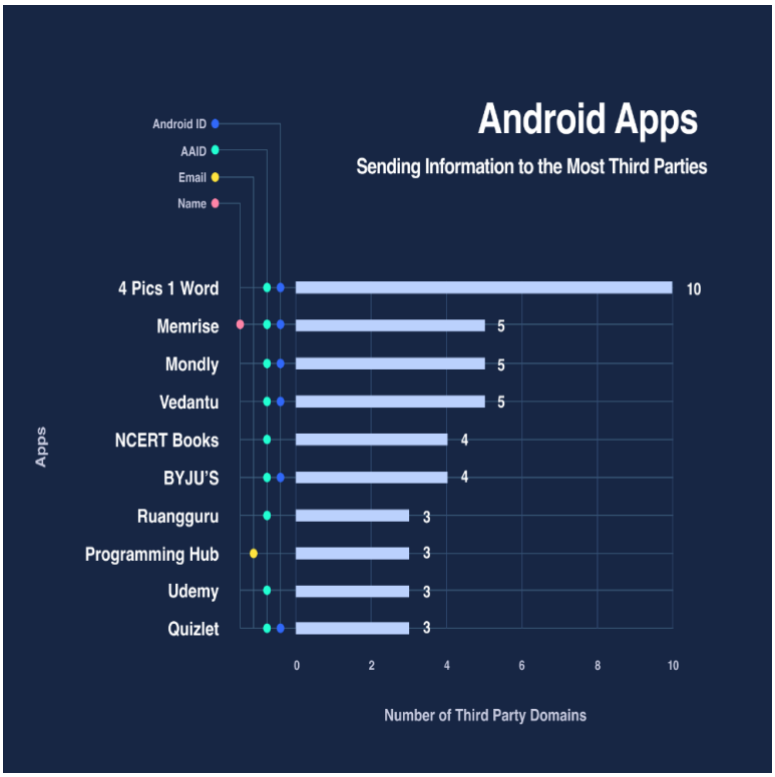

Figure 4: *The apps that communicated with the most third-parties for Android apps.*

Automated Tests

The automated test of 421 apps yielded similar results, illustrating that a few third-parties were communicating with multiple ed tech apps. Facebook, Branch.io, and Flurry communicate with -- and receive data from -- numerous apps.

IDAC contacted numerous ed tech companies prior to the publication of this report to discuss concerns about the third-party data sharing practices we observed.

We spoke to a prominent ed tech app (which claims to have over one billion installs) after our tests showed they were sharing users' AAID with Amplitude, a mobile analytics company. Our team wanted to understand why this company was sharing the AAID with Amplitude because we did not observe any ads being served while we used the app. The ed tech company in question conducted an internal assessment and concluded that it was not aware of this practice until we flagged it. The company has since halted this sharing with Amplitude. The app's assessment suggested, alarmingly, that Amplitude may be automatically collecting the AAID from Android users by default.

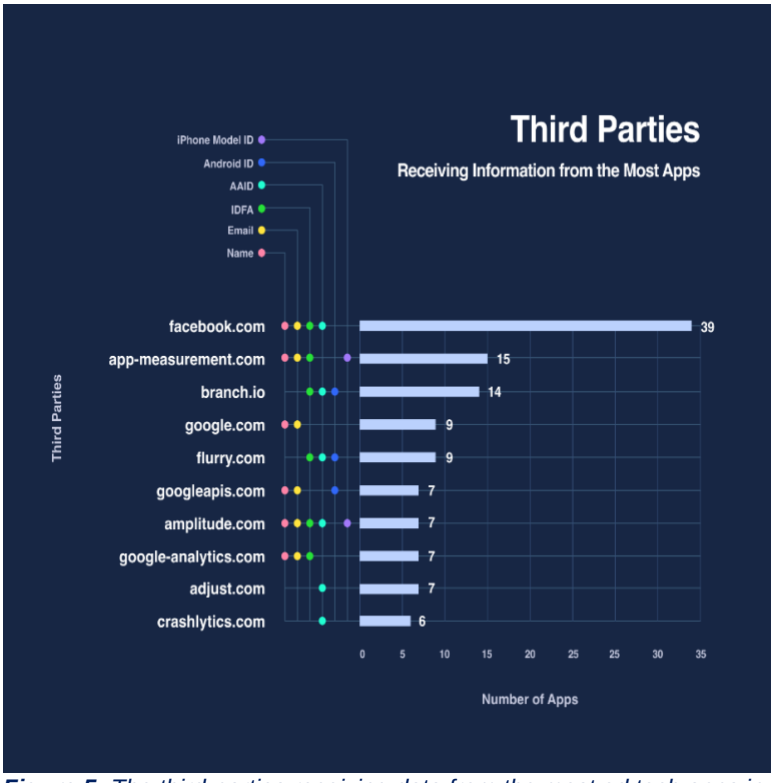

Figure 5: *The third-parties receiving data from the most ed tech apps in our manual testing pool.*

Some analytics and advertising third-parties appear to be quite aggressive with respect to their data-collection practices in the ed tech context. Moreover, it appears that in some cases developers may not be aware of the data collection that is occurring. For example, another widely-used ed tech company IDAC contacted claimed not to be aware that their app was sharing the AAID with Facebook until IDAC pointed it out. Subsequently, the ed tech company changed its practice.

Users typically do not have insight into the data protection agreements and contracts that are in place between ed tech apps and the third parties with which they contract. Without having visibility into the contractual provisions and downstream data flows, it is difficult for users to ensure that these third-parties will process users' data in ways that align with best privacy practices and users' reasonable expectations.

While some of these third-party communications are necessary for the app to function, the majority of these third-parties offer marketing, analytics, or advertisement services. By allowing these types of third-parties to access student data, apps may use that data in combination with other data to create unique user profiles for targeted and behavioral advertising purposes -- conduct that goes against best practices set forth by the Future of Privacy Forum's and the Software & Information Industry Association's Student Privacy Pledge.[16]

Our concern is that app developers may not be taking careful steps and using privacy by design principles to determine who is receiving their users' information, thereby inadvertently sharing more user data than is necessary for the app to function. By taking a minimalist approach to data sharing, developers can still accomplish their goals and do so in a manner that provides heightened privacy safeguards.

The top third-parties that received user data from ed tech apps are outlined in the table below.

Third-Party Name	Receive Data From No. of Apps
Facebook	128
Unity	72
Appsflyer	43
Mixpanel	31
Branch.io	29
OneSignal	24
MoPub	23
Applovin	20
Flurry	15

For more information refer to Appendix D.

D. ID Bridging

The troubling practice of "ID bridging" appeared to be widespread among the ed tech apps IDAC investigated. ID bridging occurs when the Android ID is sent simultaneously with the Android Advertising ID (AAID).

[16] The Student Privacy Pledge specifically states that signatories will, "Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student." https://studentprivacypledge.org/privacy-pledge.

The AAID is used to track users across apps for building an advertising profile.[17] Since 2013, Apple and Google introduced mechanisms for the advertising ID to be resettable by the user (unlike persistent IDs such as the Android ID). These resetting mechanisms give users the power, if they choose, to stop advertisers from using the users' past actions or information in future targeted ads.

Resetting the advertising ID only works if advertisers are not able to use a persistent identifier to "bridge" the old AAID and the new AAID. Bridging allows the advertiser to circumvent privacy safeguards and continue to track the user based on historical data.

Google places restrictions on the practice of ID bridging within apps. Google states that developers should, "Always respect the user's intention in resetting the advertising ID. Don't bridge user resets by using another identifier or fingerprint to link subsequent Advertising IDs together without the user's consent."[18]

Under Google's policy, developers can share *either* the Android ID *or* the AAID (depending on the nature of the third-party service), but not both together. This minimization technique helps prevent third-parties from being able to bridge AAIDs across resets.

We observed the practice of ID bridging by ed tech apps in both our manual and automated tests.

Manual Tests

We found the Android ID being sent simultaneously with the AAID in 15 apps during our manual tests. It is not readily apparent why this is occurring; however, collecting these identifiers together can enable an app to bypass a device's privacy settings that the user had previously set. The fact that 15 out of the 78 Android apps we tested engaged in this conduct suggests that this is more common than anticipated.

Our team found no potential cases of ID bridging performed on the iOS apps, in which the IDFA would be sent next to a persistent identifier, such as SEID[19] or IMEI[20].

The table below demonstrates the nine most popular apps that were observed engaging in ID bridging by sending the Android ID and AAID together to third-parties.[21] Each of these nine apps had at least 10 million installs on the Google Play Store.

App Name	Third-Party Receiving AAID & Android ID
Brainly – The Homework App	Branch.io
Hello English: Learn English	Flurry.com

17 https://digitalwatchdog.org/trend-report-apps-oversharing-your-advertising-id

18 https://developer.android.com/training/articles/user-data-ids

19 The SEID, or Secure Element Identifier, is a piece of data contained within the Near-Field Communication chip in the phone (which is used, among other functions, for Apple Pay).

20 The IMEI, or International Mobile Equipment Identity, is a unique identifier for certain models of mobile phones.

21 We also observed a few apps sending both the Android ID and the AAID to Segment, but we excluded Segment's service from the above list because Segment acts as a remote first-party server, allowing companies to securely store their data.

Learn 33 Languages Free - Mondly	Flurry.com
BYJU'S – The Learning App	Appsflyer.com, Byjus.com, Tllms.com
Kobo Books - eBooks & Audiobooks	Branch.io
ISS Live Now: Live HD Earth View and ISS Tracker	Flurry.com
Quizlet: Learn Languages & Vocab with Flashcards	Branch.io, Facebook.com, Googleadservices.com
Vedantu: LIVE Learning App | Class 1-12, JEE, NEET	Branch.io, Moengage.com
4 Pics 1 Word	Adjoe.zone, Branch.io

Automated Tests

The automated tests we ran on the broader group of 421 Android ed tech apps confirm that ID bridging is widespread in ed tech apps. 203 apps were observed collecting and sharing the Android ID and the AAID together. We found a total of 233 third-parties that receive this data.

The table below highlights seven popular apps that were observed performing this ID bridging in transmissions to third-parties. Each app has at least 10 million installs on the Google Play Store.

App Name	Third-Party Receiving AAID & Android ID
Rosetta Stone: Learn Languages	Facebook.com, Programminghub.io
NeuroNation - Brain Training & Brain Games	Appfour.com
BYJU'S – The Learning App	Doubtnut.com, Branch.io, Moengage.com, Appsflyer.com, Apxor.com, Googleadservices.com
Duolingo: Learn Languages Free	Facebook.com, Newrelic.com
HelloTalk — Chat, Speak & Learn Foreign Languages	Bugtags.cn, Taobao.com, Ready4.com, Aliyuncs.com, Facebook.com, Umeng.com
Photomath	Redditmedia.com, Redd.it, Reddit.com
SkyView® Lite	Facebook.com

The table below demonstrates the top third-parties that receive users' Android ID and AAID together.

Domain	App Count
facebook.com	68
crashlytics.com	66
googleapis.com	53
doubleclick.net	44
googleadservices.com	42
google.com	28
mixpanel.com	14
mopub.com	12
branch.io	10
gstatic.com	10
appsflyer.com	9
adjust.com	9
unity3d.com	9
onesignal.com	9
amazonaws.com	9
googleusercontent.com	8
flurry.com	8
braze.com	7
amazon-adsystem.com	7
cloudfront.net	7

For more information refer to Appendix E.

E. Software Development Kits

IDAC also had some concerns about privacy risks created by the use of software development kits (SDKs) in connection with some ed tech apps.

Third-party SDKs are pieces of code that developers embed in their apps to perform a specific task or function. SDKs are convenient tools for developers since they can provide useful services (e.g., provide user interface layout, send push notifications, text-to speech processing, etc.).

SDKs are commonly used and their presence does not automatically create a concern. However, we believe that the presence of certain SDKs in some ed tech apps warrants further scrutiny.

In particular, there are privacy risks associated with some analytics, advertisement, and social network SDKs in the ed tech context. These kinds of SDKs raise particular concerns because of their data collection and sharing practices, as well as their monetization functionalities. Analytics, advertisement, and social network SDKs may be appropriate in certain circumstances, but we recommend that ed tech app developers take caution when using these types of SDKs.

We also suggest that developers take particular care to be transparent about what third-party SDKs are embedded in their apps. Many privacy policies do not disclose which third-party SDKs are embedded within an app. This lack of transparency deprives parents and educators of the tools they need to assess the privacy risks posed by ed tech apps using these third party SDKs.

Developers should only include SDKs when the associated functionality is necessary and appropriate. Context matters.

Moreover, it is particularly concerning when apps with aggressive SDKs request permissions that Google classifies as "dangerous."[22] Because permissions occur at the app level, a user could, for example, grant the app permission to access user's for a legitimate purpose, but then inadvertently allow an aggressive SDK to also access that location data.

Mobile analytics and advertising SDKs pose particular risks in ed tech apps -- especially apps that have younger users -- because of their monetization capabilities.

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

Additionally, SDKs that provide multiple functionalities such as advertising and analytics ("mixed purpose SDKs") present particular challenges. To prevent the unintentional transmission of users' personal data to third-parties, developers should ensure that they only use the components of the SDK that they actually need. The components of these SDKs that do not relate to needed functionality should be disabled.

Fully 46% of the apps we tested used a potentially concerning SDK. It is possible that developers use these third-party SDKs out of convenience without understanding how the SDKs function within their app. Regardless of the reasons for the presence of these privacy risks, developers should take greater care to ensure that user data is not being misused. As discussed in Section C, we observed SDKs collecting users' data by default, sometimes without the developer's awareness.

The table below highlights the four Android apps that use the greatest number of flagged SDKs.

App Name	Flagged SDK Count	Social Network SDKs	Mobile Analytics SDKs	Advertisement SDKs
Hello English: Learn English	5	--	Flurry, Flurry SDK	Google Ads, Supersonic Ads, Unity3d Ads
BrainPOP ELL	3	--	Google Analytics, Google Tag Manager, HockeyApp	--

[22] https://developer.android.com/guide/topics/permissions/overview

Learn 33 Languages Free - Mondly	3	Facebook, Twitter	Crashlytics	--
Coursera: Online courses	3	Tencent Login, Facebook	Crashlytics	--

For more information refer to Appendix F.

II. IDAC Recommendations

In order to promote trust and help parents, teachers, and schools that are more widely adopting ed tech apps during the COVID-19 pandemic, developers and companies can take additional steps to mitigate risk and follow best practices in this space. Based on the research we outlined in this report, we recommend the following:

Location and Device Identifier Collecting and Sharing. Unless absolutely necessary for the app to provide its services, developers should refrain from collecting and sharing location data and persistent identifiers.

Transparency. When ed tech apps collect location information and/or persistent identifiers, developers should be transparent in their privacy policies about collecting this information.

Personal Data Exposure in URL Query Strings. To mitigate the risk of a security attack or unauthorized access to data, developers should follow best practices and review URLs to ensure that no personal data is being transmitted.

Third-Party Communications. Data sharing is always a privacy concern, but it is especially heightened when children's information is implicated. In order to protect users' privacy, developers should prioritize privacy by design principles such as data minimization. Ed tech apps should limit the information they collect about users, as well as which third-parties receive data.

Contractual Safeguards and Privacy Controls. To the extent that ed tech companies share personal data with third parties, they should ensure that there are contractual safeguards and privacy controls in place.

ID Bridging. Apps can track users across AAID resets when they collect the Android ID and AAID together, bypassing privacy safeguards put in place by Google. We recommend that app developers stop sharing the Android ID for advertising purposes. We also strongly advise against collecting and sharing both the AAID and Android ID together. It is best to determine which identifier is appropriate for the service and only share that identifier when necessary.

Software Development Kits. Developers should carefully review third-party SDKs to understand how they interact with apps and ensure they are not collecting more data than is authorized. Avoid using SDKs that are not transparent about what data they collect and share. Lastly, check the SDK to see if it collects user data by default, and if so, reconfigure the SDK if necessary.

Ed tech companies must be transparent about their privacy practices. To promote the use of these apps, users must be made aware of what information they are providing and the purposes for which it is collected. Parents and schools must feel comfortable that their students' privacy is not being compromised. By taking these additional measures, ed tech companies and developers can help improve student privacy in the mobile app ecosystem.

Appendices